Enterasys®

Network Access Control

Design Guide

P/N 9034385

enterasys®

Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810

Part Number: 9034385 March 2008

Documentation URL: http://www.enterasys.com/support/manuals

Documentacion URL: http://www.enterasys.com/support/manuals

Dokumentation im Internet: http://www.enterasys.com/support/manuals

Contents

About This Guide

Chapter 1: Overview

Chapter 2: NAC Deployment Models

Chapter 3: Use Scenarios

Chapter 4: Design Planning

Chapter 5: Design Procedures

Figures

Tables

About This Guide

The NAC Design Guide describes the technical considerations for the planning and design of the Enterasys Network Access Control (NAC) solution. The guide includes the following information:

For information about...	Refer to...
An overview of the Enterasys NAC Solution and a comparison between the inline NAC Controller and the out-of-band NAC Gateway appliances.	Chapter 1, **Overview**
The four different NAC deployment models and their requirements.	Chapter 2, **NAC Deployment Models**
Four NAC use scenarios that demonstrate the deployment of inline versus out-of-band network access control.	Chapter 3, **Use Scenarios**
Design planning steps including identifying your deployment model, evaluating your infrastructure requirements, and deciding whether to deploy inline versus out-of-band NAC.	Chapter 4, **Design Planning**
Design procedures and considerations for deploying both out-of-band and inline NAC on an enterprise network.	Chapter 5, **Design Procedures**

Intended Audience

This document is intended for experienced network administrators who are responsible for designing and implementing network access control on their network.

Related Documents

Before reading this design guide, Enterasys recommends that you read the Enterasys Network Access Control Whitepaper available at the following website:

http://www.enterasys.com/company/literature/nac-wp.pdf

The manuals listed below provide additional information regarding the Enterasys NAC solution. They are available in Adobe Acrobat Portable Document Format (PDF) at the following website:

http://www.enterasys.com/support/manuals

- *NAC Controller Hardware Installation Guide* provides product descriptions and installation instructions for the NAC Controller.
- *NAC Gateway Appliance Installation Guide* for the installation of the Enterasys NAC Gateway SNS-TAG-HPA and SNS-TAG-LPA hardware appliances.
- *NAC Gateway Appliance Installation Guide* for the installation of the Enterasys NAC Gateway SNS-TAG-ITA hardware appliance.

- Enterasys NAC Manager Online Help. Explains how to use NAC Manager to configure your NAC appliances, and to put in place authentication and assessment requirements for the end-systems accessing your network.
- *Installing the Assessment Agent on the Lockdown Enforcer Appliance*. Provides instructions for installing the Enterasys Networks Assessment Agent on the Lockdown Enforcer appliance (or another Linux system). The Assessment Agent is required for communication between the NAC appliance and the Lockdown Enforcer appliance.
- *Installing the Assessment Agent on the Nessus Server*. Provides instructions for installing the Enterasys Networks Assessment Agent on the Nessus server. The Assessment Agent is required for communication between the NAC appliance and the Nessus server.

Getting Help

For additional support related to NAC products or this document, contact Enterasys Networks using one of the following methods:

World Wide Web	www.enterasys.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-978-684-1000 To find the Enterasys Networks Support toll-free number in your country: www.enterasys.com/support
Internet mail	support@enterasys.com To expedite your message, type **[NetSight]** in the subject line.

To send comments concerning this document to the Technical Publications Department:

techpubs@enterasys.com

Please include the document Part Number in your email message.

Before contacting Enterasys Networks for technical support, have the following data ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

1

Overview

This chapter provides an overview of the Enterasys Network Access Control (NAC) solution, including a description of key NAC functions and deployment models. It also introduces the required and optional components of the Enterasys NAC solution, and presents a comparison between the inline NAC Controller for implementation of inline network access control and the out-of-band NAC Gateway for implementation of out-of-band network access control.

NAC Solution Overview

Enterasys NAC is a centralized network access control solution that combines authentication, vulnerability assessment, and location services to authorize network access and determine the appropriate level of service for an end-system. The NAC solution ensures that only valid users and devices connecting at the proper location, at the right time, and with appropriate security postures, are granted access to your network. For end-systems which are not compliant with defined security guidelines, the NAC solution provides assisted remediation, allowing end users to perform self-service repair steps specific to the detected compliance violation.

Key Functionality

The Enterasys NAC solution supports the five key network access control functions: detection, authentication, assessment, authorization, and remediation. These five functions can be deployed in various combinations, as described in the following section on deployment models.

Here is a description of the five key NAC functions:

Detection

Identify when and where a device connects to the network.

Authentication

Verify the identity of the user or device connecting to the network. Enterasys NAC supports the “pass through” authentication (proxying to a backend RADIUS server) of 802.1X, web-based (PWA), and MAC authentication requests, as well as local MAC authentication. This provides access control for both user-centric and machine-centric end-systems in the enterprise environment.

Assessment

Determine if the device complies with corporate security and configuration requirements, such as operating system patch revision levels and antivirus signature definitions. Other security compliance requirements might include the physical location of the device and the time of day the connection attempt is made.

Authorization

Determine the appropriate network access for the connecting device based on the authentication and/or assessment results, and enforce this authorization level to the end-system. The authorization level can be determined based on the device's location, MAC address, and security posture (as determined by the assessment results), in addition to the identity of the user/device validated through authentication.

The end-system can be authorized for network access using different techniques, such as reconfiguring access edge switches or leveraging a specialized NAC appliance deployed in the transmission path of end-system data traffic. Inline and out-of-band NAC implementations use different techniques for authorizing end-systems on the network, each with unique advantages and disadvantages as discussed later in this chapter.

Remediation

Enable end users to safely remediate their non-compliant end-systems without impacting IT operations. With remediation, users can be notified when their system is quarantined for network security policy non-compliance, and they can be directed to perform self-service remediation techniques specific to the detected compliance violation. Notification methods include web redirection via a captive portal, email notification, pop-up messages, and messenger service integration, among others.

The remediation process includes updating the device to meet corporate security requirements (for example, updating operating system patches and antivirus signatures) and reinitiating the network access process. Network resources can be automatically reallocated to end-systems that have successfully performed the remediation steps, without the intervention of IT operations.

Deployment Models

The five key NAC functions described above do not need to be implemented concurrently in a NAC deployment. For example, to support MAC registration for guests and other users on the network, the detection, authentication, and authorization functionalities can be implemented without the assessment functionality. This allows an IT department to gain visibility into who is using which devices on the network while allowing only valid users to enter the network.

As another example, the assessment functionality can be added to the detection, authentication, and authorization of end-systems without the remediation functionality, allowing for the auditing, but not quarantining, of connecting end-systems. This provides visibility into the security posture and configuration of connecting end-systems without impacting device network connectivity, and can be used for auditing and software update purposes by the IT department.

The four NAC deployment models described below build on each other by implementing subsets of the five key NAC functions. Each model provides particular aspects of NAC functionality, supporting the requirements of diverse enterprise environments. With each subsequent model, the additional NAC functionality can be enabled without the need to replace pieces of the Enterasys NAC solution.

Model 1: End-system Detection and Tracking

This NAC deployment model implements the *detection* piece of NAC functionality. It supports the ability to track users and end-systems over time by identifying where they are currently connected to the network and where they have connected to the network at any given time in the past. This information is useful for compliance and auditing purposes, as well as other management operations that require complete visibility into the current and historical connections of end-systems and users.

Model 2: End-System Authorization

This NAC deployment model implements the *detection*, *authentication*, and *authorization* NAC functionalities, to control access to network resources based on user and end-system identity and location. The model supports MAC address or guest registration, where new end-systems are forced to provide a valid user identity in a web page form before being allowed access to the network. Following successful registration, end-systems are granted measured access, without requiring the intervention of network operations.

Model 3: End-System Authorization with Assessment

This NAC deployment model implements the *detection*, *authentication*, *assessment*, and *authorization* NAC functionalities, to control access to network resources based on the security posture of a connecting end-system, as well as user and device identity and location. End-systems that fail assessment can be dynamically quarantined with restrictive network access to mitigate the propagation of security threats on the network, while compliant end-systems are permitted onto the network with a measured level of access.

Alternatively, specific end-systems and users can be assessed upon network connection and be permitted network access regardless of the assessment results. This approach allows an IT administrator to have visibility into the configuration of end devices on the network without impacting their network connectivity during or after assessment. This approach is usually implemented during the initial rollout of the NAC solution for baselining purposes.

This NAC deployment model requires the use of either integrated assessment server functionality or the ability to connect to external assessment services, in order to execute the end-system vulnerability assessment.

Model 4: End-System Authorization with Assessment and Remediation

This NAC deployment model implements the *detection*, *authentication*, *assessment*, *authorization*, and *remediation* NAC functionalities, providing for the quarantine and remediation of noncompliant devices. Assisted remediation uses web-based notification to dynamically inform quarantined end-systems of security compliance violations, and allow end users to safely remediate their quarantined end-system without impacting IT operations.

NAC Solution Components

This section discusses the required and optional components of the Enterasys NAC solution, beginning with the following table that summarizes the component requirements for each of the four deployment models.

Table 1-1 Component Requirements for NAC Deployment Models

NAC Component	Model 1 Detection and Tracking	Model 2 Authorization	Model 3 Authorization with Assessment	Model 4 Authorization with Assessment and Remediation
NAC Appliance	Required	Required	Required	Required
NetSight NAC Manager	Required	Required	Required	Required
NetSight Console	Required	Required	Required	Required
Assessment Server	*Optional*	*Optional*	Required	Required
RADIUS Server[1]	*Optional*	*Optional*	*Optional*	*Optional*
NetSight Policy Manager[2]	*Optional*	*Optional*	*Optional*	*Optional*
NetSight Inventory Manager[3]	*Optional*	*Optional*	*Optional*	*Optional*

[1] A RADIUS server is only required if out-of-band NAC is implemented with the NAC Gateway, and 802.1X or web-based authentication is deployed on the network.

[2] NetSight Policy Manager is required for inline NAC deployments. NetSight Policy Manager is suggested if Enterasys policy-capable switches are deployed on the network and utilized as the traffic enforcement or authorization point for connecting devices. Policy Manager allows the centralized definition and deployment of policies to Enterasys switches for the consistency and ease of management of the authorization levels for connecting end-systems.

[3] NetSight Inventory Manager is suggested if Enterasys switches are deployed on the network for ease of firmware and configuration management across the enterprise.

The NAC Appliance

The NAC appliance is a core component of the Enterasys NAC solution and is required for all NAC deployment models. It provides the ability to detect, authenticate, and effect the authorization of end devices attempting to connect to the network. It also integrates with or connects to assessment services to determine the security posture of end-systems connecting to the network. Once authentication and assessment are complete, the NAC appliance effects the authorization of devices on the network by allocating the appropriate network resources to the end-system based on authentication and/or assessment results.

If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC appliance can deny the end-system access to the network, quarantine the end-system with a highly restrictive set of network resources, or permit network access, depending on the appliance’s configuration.

The NAC appliance also provides the remediation functionality by means of a Remediation Web Server that runs on the appliance. Remediation informs end users when their end-systems have been quarantined due to network security policy non-compliance, and allows end users to safely remediate their end-systems without assistance from IT operations.

Enterasys offers two types of NAC appliances: the NAC Gateway appliance implements out-of-band network access control, and the NAC Controller appliance implements inline network access control. The following section describes how each NAC appliance implements network access control for connecting end-systems.

NAC Gateway Appliance

The NAC Gateway is utilized to implement out-of-band network access control for connecting end-systems. With the NAC Gateway, connecting end-systems are detected on the network through their RADIUS authentication interchange. Based on the assessment and authentication results for a connecting device, RADIUS attributes are added or modified during the authentication process to authorize the end-system on the authenticating edge switch. Therefore, the NAC Gateway can be positioned anywhere in the network topology with the only requirement being that IP connectivity between the authenticating edge switches and the NAC Gateways is operational.

The NAC Gateway requires the implementation of intelligent wired or wireless edge infrastructure devices as the authorization point for connecting end-systems. Intelligent edge devices are capable of supporting authentication and authorization based on the authentication message interchange. Depending on the appliance model, the NAC Gateway provides either integrated assessment server functionality and/or the ability to connect to external assessment services, to determine the security posture of end-systems connecting to the network.

Three NAC Gateway models are available to meet the needs of different-sized implementations and assessment server requirements.

- **SNS-TAG-ITA** supports up to 3000 concurrent end-systems and provides integrated assessment servers. (A separate license is required for integrated assessment.) This integrated NAC Gateway supports both agent-less (network-based) and agent-based assessment. In addition to having the capability to run as an integrated appliance, it also has the capability to run as an assessment server (scanner) only. The SNS-TAG-ITA also supports the ability to connect to multiple external assessment servers including Nessus and Lockdown Enforcer.
- **SNS-TAG-HPA** supports up to 3000 concurrent end-systems and supports the ability to connect to multiple external assessment servers including Nessus and Lockdown Enforcer.
- **SNS-TAG-LPA** supports up to 2000 concurrent end-systems and supports the ability to connect to multiple external assessment servers including Nessus and Lockdown Enforcer.

NAC Controller Appliance

The NAC Controller is utilized to implement inline network access control for connecting end-systems. With the NAC Controller, connecting end-systems are detected through the receipt of a packet from a new end-system. Based on the assessment and authentication results for a connecting device, the authorization of the end-system is implemented locally on the NAC Controller appliance by assigning a set of traffic forwarding rules, referred to as “policy,” to all traffic sourced by the end-system. The NAC Controller appliance is positioned strategically in the network topology within the end user LAN segment or across routed boundaries, inline with data traffic sourced from end-systems. Since this appliance exists in the data path of networked devices, it has been designed to achieve multi-gigabit throughput with hardware-based traffic forwarding, by leveraging customized Enterasys-built Application Specific Integrated Circuits (ASICs).

The NAC Controller is applicable to scenarios where non-intelligent wired or wireless edge infrastructure devices are deployed in the network. Non-intelligent edge devices are not capable of supporting authentication and/or authorization. The NAC Controller is also required in IPSec and SSL VPN deployments.

The NAC Controller provides integrated vulnerability assessment server functionality and supports both agent-less (network-based) and agent-based assessment. (A separate license is required for integrated assessment.) It also supports the ability to connect to multiple external assessment servers including Nessus and Lockdown Enforcer.

The NAC Controller can be configured in one of two modes of operation: Layer 2 or Layer 3. The mode of operation controls how connecting end-systems are detected by the NAC Controller on the network and is selected based on where the NAC Controller is positioned in the network in relation to these end-systems. If the NAC Controller is positioned before the first routed boundary for connecting end-systems, closer to the access edge of the network, the Layer 2 NAC Controller mode is utilized. In this mode of operation, the NAC Controller detects connecting end-systems on the network by receiving traffic from a new MAC address. If the NAC Controller is positioned after the first routed boundary deeper inside the network, the Layer 3 NAC Controller mode is utilized. In this mode of operation, the NAC Controller detects connecting end-systems on the network by receiving traffic from a new IP address. With the NAC Controller supporting both Layer 2 and Layer 3 modes of operation, the NAC Controller can be strategically positioned in the network topology to achieve the desired level of scalability and security.

The NAC Controller is available in two models:

- **2S4082-25-SYS - 24-Port 10/100/1000 NAC Controller** supports up to 2000 concurrent end-systems.
- **7S4280-19-SYS - 18-Port SFP NAC Controller** supports up to 2000 concurrent end-systems.

Appliance Comparison

The following table compares how the two NAC appliance types implement the five NAC functions.

Table 1-2 Comparison of Appliance Functionality

NAC Function	NAC Gateway	NAC Controller
Detection	RADIUS authentication request is received from access edge switches.	Traffic sourced from a new end-system traverses the inline appliance.
Authentication	For user authentication, RADIUS authentication requests are proxied to an upstream RADIUS server which contains a database of valid user credentials. For device authentication, the NAC Gateway can locally validate whether the connecting MAC address is permitted network access.	It is possible to disable authentication on the NAC Controller and rely instead on the authentication of the end-system by downstream infrastructure devices, such as authenticating to a wireless LAN or VPN concentrator. Alternatively, the NAC Controller supports MAC registration where the end user must provide a valid username and password, verified via LDAP, before being allowed to register to the network.
Assessment	Assessment can be implemented using localized, integrated agent-based and/or agent-less assessment[1] or external agent-based and/or agent-less assessment using a bank of external assessment servers (Nessus and Lockdown Enforcer) for maximum assessment scalability. The SNS-TAG-ITA Gateway appliance provides integrated assessment servers.	Assessment can be implemented using localized, integrated agent-based and/or agent-less assessment[1] or external agent-based and/or agent-less assessment using a bank of external assessment servers (Nessus and Lockdown Enforcer) for maximum assessment scalability.
Authorization	For Enterasys access edge switches, the end-system is assigned a policy (a set of granular traffic forwarding rules) and/or VLAN based on the authentication and assessment results. For third-party edge switches, the end-system is assigned a VLAN via RFC 3580 Tunnel attributes based on the authentication and assessment results.	End-system's traffic is assigned a policy (a set of granular traffic forwarding rules) at the NAC Controller, based on authentication and assessment results.
Remediation	Captive web portal is served by the NAC Gateway.	Captive web portal is served by the NAC Controller.

[1] A separate license for integrated assessment functionality is required.

Table 1-3 outlines the advantages and disadvantages of the two appliance types as they pertain to network security, scalability, and configuration/implementation.

Table 1-3 Comparison of Appliance Advantages and Disadvantages

Features	NAC Gateway	NAC Controller
Supported Connection Types	**Disadvantage:** Restricted to wired and wireless access edge with authentication and authorization functionality.	**Advantage:** Flexible, catering to wired and wireless access edge as well as remote access VPN of any type.
Deployment	**Advantage:** Less disruptive because no topology reconfiguration is required.	**Disadvantage:** More disruptive because topology reconfigurations are required to place the NAC Controller inline with data traffic on the network.
Configuration	**Disadvantage:** More complex because the NAC Gateway requires that an authentication method is deployed on the network, and that the authenticating access edge switches are capable of dynamically authorizing end-systems based on the RADIUS authentication interchange.	**Advantage:** Less complex because there is no dependency on authentication and downstream infrastructure device functionality.
Security	**Advantage:** More secure because the traffic enforcement point for end-system authorization is closer to the end-system's port of network connection on the access layer switch. Therefore, an offending end-system poses a threat to a smaller set of network resources.	**Disadvantage:** The authorization point is farther from the end-system point of connection. An offending end-system poses a threat to all network resources downstream from the NAC Controller because the traffic enforcement point is implemented at the inline NAC appliance. Malicious traffic will be discarded only when an end-system communicates through the appliance.

Table 1-3 Comparison of Appliance Advantages and Disadvantages (continued)

Features	NAC Gateway	NAC Controller
NAC Granularity	**Advantage:** The NAC Gateway is always aware of the MAC address of the device connecting to the network, and its associated IP address, username, and location (switch IP address and port). Therefore, NAC can be configured to uniquely authenticate, assess, and authorize specific end-systems and users in particular locations in the network.	**Disadvantage:** While the Layer 2 NAC Controller knows the MAC address of the connecting end-system and can obtain the associated username, the Layer 3 NAC Controller may not have this information. Therefore, the Layer 3 NAC Controller lacks the ability to uniquely authenticate, assess, and authorize specific devices and users, and implements NAC for all connected end-systems in the same way. Furthermore, Layer 2 and Layer 3 NAC Controllers do not provide visibility down to the access layer port to which an end-system is connected, and cannot control access to the network based on switch access layer port connection.
Scalability	**Advantage:** Very scalable because little if any end-system data traffic is processed by the NAC Gateway (being out-of-band). Therefore, an increased number of end-systems are supported per NAC Gateway.	**Advantage:** Very scalable because hardware-based forwarding of data traffic using Enterasys-built custom ASICs is implemented to achieve multi-gigabit throughput speeds for the NAC Controller.

NetSight Management

The NAC appliances are configured, monitored, and managed through management applications within the Enterasys NetSight Suite. NetSight is a family of products comprised of NetSight Console and a suite of plugin applications. Of the following NetSight applications, NetSight NAC Manager and NetSight Console are required for all four NAC deployment models, while NetSight Policy Manager and NetSight Inventory Manager are optional, depending on your network configuration and the network access control features you wish to implement. Following is a description of the NetSight applications.

NetSight NAC Manager

NetSight NAC Manager is a required core component in the Enterasys NAC solution. NAC Manager and NAC appliances work in conjunction to implement network access control. NAC Manager provides configurations for the assessment, authentication, authorization, and remediation parameters for all NAC appliances (NAC Gateways and NAC Controllers) from one centralized interface. After these configurations are enforced, the NAC appliances can detect, authenticate, assess, authorize, and remediate end-systems connecting to the network according to those configuration specifications.

NetSight Console

NetSight Console is used to monitor the health and status of infrastructure devices in the network, including switches, routers, Enterasys NAC appliances (NAC Gateways and NAC Controllers) as well as other security appliances. NetSight NAC Manager is a plugin to NetSight Console, and NetSight Console must be installed on a server with NAC Manager for the Enterasys NAC solution.

NetSight Policy Manager

The NetSight Policy Manager application provides the ability to centrally define and configure the authorization levels or “policies” for certain NAC deployments. Policy Manager is required for inline NAC deployments, and provides the ability to configure and manage policies on the NAC Controller appliance. Policy Manager is recommended for out-of-band NAC deployments that include Enterasys policy-enabled switches in the access layer, and provides the ability to centrally manage policies on these switches. This central administration of policies using Policy Manager includes distribution of the “Enterprise User,” “Assessing,” “Quarantine,” and “Failsafe” policy roles to the policy enforcement points.

NetSight Inventory Manager

The NetSight Inventory Manager application is an optional component of the NAC solution, providing comprehensive network inventory and change management capabilities for your network infrastructure.

RADIUS Server

A RADIUS server with backend directory services must be implemented in the NAC solution if 802.1X or web-based (PWA) authentication of end-systems is utilized with out-of-band network access control.

Furthermore, if RADIUS is utilized for authenticating management logins for infrastructure devices, a RADIUS server must be deployed on the network.

Assessment Server

If the NAC deployment model includes vulnerability assessment, one or more assessment servers must be deployed on the enterprise network either as integrated components of the NAC appliance or as external assessment services.

Summary

The Enterasys NAC solution supports the five key network access control functions: detection, authentication, assessment, authorization, and remediation. Four NAC deployment models provide support for diverse enterprise environments, with each model implementing particular aspects of NAC functionality.

- Model 1: End-System Detection and Tracking - Implements *detection* to provide visibility into what devices are connecting to the network, who is using these devices, and where the devices are connected.
- Model 2: End-System Authorization - Implements *detection*, *authentication*, and *authorization* to provide network access control based on user and end-system identity and location.

- Model 3: End-System Authorization with Assessment - Implements *detection*, *authentication*, *assessment*, and *authorization* to provide network access control based on the security posture of a connecting end-system, as well as user and device identity and location. This model requires the use of either integrated assessment server functionality or the ability to connect to external assessment services, in order to perform the end-system assessment.
- Model 4: End-System Authorization with Assessment and Remediation - Implements *detection*, *authentication*, *assessment*, *authorization*, and *remediation*, providing the additional ability to quarantine and remediate noncompliant devices.

The NAC appliance is a core component of the Enterasys NAC solution and is required for all NAC deployment models. It provides the ability to detect, authenticate, and authorize end devices attempting to connect to the network. It also integrates with or connects to assessment services to perform assessment of end-systems connecting to the network. Once authentication and assessment are complete, the NAC appliance authorizes devices on the network by allocating the appropriate network resources to the end-system based on authentication and/or assessment results. The NAC appliance also provides remediation functionality, allowing end users to safely remediate their quarantined end-system without impacting IT operations.

Enterasys offers two types of NAC appliances:

- The NAC Gateway appliance implements out-of-band network access control and requires the implementation of intelligent wired or wireless edge infrastructure devices on the network.
- The NAC Controller appliance implements inline network access control and is applicable to scenarios where non-intelligent wired or wireless edge infrastructure devices are deployed in the network. The NAC Controller is also required in IPSec and SSL VPN deployments.

The NAC appliances are configured, monitored, and managed through Enterasys NetSight management applications. NetSight NAC Manager and NetSight Console are required for all four NAC deployment models. NAC Manager provides configurations for the assessment, authentication, authorization, and remediation parameters for all NAC appliances, while NetSight Console is used to monitor the health and status of infrastructure devices in the network, including switches, routers, and Enterasys NAC appliances.

NetSight Policy Manager and NetSight Inventory Manager are optional NetSight applications. Policy Manager provides the ability to centrally define and configure the authorization levels or “policies” for certain out-of-band NAC deployments and all inline NAC deployments. Inventory Manager provides comprehensive network inventory and change management capabilities for your network infrastructure.

The next chapter provides a more detailed description of the four NAC deployment models including their requirements and implementation.

2

NAC Deployment Models

This chapter describes the four NAC deployment models and how they build on each other to provide a complete NAC solution. The first model implements a subset of the five key NAC functions (as described in Chapter 1), and each subsequent model provides additional functionality without the need to replace existing pieces of the NAC solution. This allows businesses who are still in the early stages of NAC deployment, to take a phased approach to implementing NAC while deriving value from the solution at each step along the way.

Model 1: End-System Detection and Tracking

This NAC deployment model implements the first key NAC function, detection. The detection of connecting end-systems provides the network administrator with visibility into what devices are connecting to the network, who is using these devices, and where the devices are connected.

For many NAC deployments, the first phase consists of tracking over time the end-systems and end users connected to the network, in order to profile and enumerate the assets on the enterprise network. It is important to note that in this model, the NAC solution does not play a part in authorizing access for connecting end-systems, leaving this to the default configurations on the switch. The end-systems connect to the network and are allocated “business-as-usual” access to network resources, while the NAC solution provides visibility into the connection behavior and details of these devices.

Implementation

End-systems can be detected and tracked in different ways depending on whether inline or out-of-band network access control is implemented.

Out-of-Band NAC

For out-of-band NAC utilizing the NAC Gateway appliance, detection is implemented as follows. In the case of web-based or 802.1X authentication, end-systems are detected with the receipt of RADIUS packets from an access edge switch attempting to authenticate an end-system. The

RADIUS Access-Accept or Access-Reject message received from the upstream RADIUS server, is returned without modification to the access edge switch, to permit end-system access to the network. For MAC authentication, a RADIUS Access-Accept message is returned to the access edge switch without modification, based on a RADIUS Access-Accept message received from the upstream RADIUS server or local authorization of MAC authentication requests. The authenticating end-system is provided access to the network based on the configuration of the access edge switch.

Inline NAC (Layer 2)

For inline NAC utilizing the Layer 2 NAC Controller, an end-system can be detected in multiple ways. An end-system can be detected simply by transmitting data traffic not previously seen by the NAC controller. In this case, the traffic is forwarded through the NAC Controller to the traffic destination, and has no impact on the connectivity of the end-system. In another method, end-systems are detected with the authentication of downstream end-systems via 802.1X, web-based, and/or MAC authentication on the NAC Controller. These authentication requests may or may not be proxied upstream depending on the NAC configuration.

Inline NAC (Layer 3)

For inline NAC utilizing the Layer 3 NAC Controller, an end-system is detected simply by transmitting data traffic sourced from an IP address not previously seen by the NAC controller. The traffic is forwarded through the NAC controller to the traffic destination, and has no impact on the connectivity of the end-system.

Features and Value

There are two key pieces of functionality and value propositions supported by Model 1:

End-System and User Tracking

Model 1 supports the ability to track end-systems by MAC address, as the device moves from switch port to switch port, and map the device identity to its IP address every time it connects. Furthermore, the associated user can also be mapped to the device and IP address, as long as a username-based authentication method (802.1X or web-based authentication) or MAC Registration is implemented with the NAC Gateway, or if end users are configured to login to a Microsoft Windows domain with the NAC Controller using Kerberos snooping functionality.

Using these methods, the Enterasys NAC solution can identify who, what, when, and where devices and users connect to the network. This information is maintained centrally in the NetSight NAC Manager database, providing important historical data that can be used for auditing or troubleshooting purposes. In addition, this information can be easily searched to identify which port a particular user is currently connected to on the network, or which device is currently allocated a particular IP address. This binding (IP address, MAC address, username, location), which is maintained over time for each end-system, is useful for compliance and auditing purposes, and for planning the subsequent rollout of the next NAC deployment model.

IP-to-ID functionality for Security Information Management (SIM)

This NAC deployment model enables SIM systems such as the Enterasys Dragon Security Command Console (DSCC), to display user-focused information about assets on the network. Traditionally, SIM systems yield device-focused information (such as IP address) about detected network threats, through the correlation, normalization, and prioritization of events and information on the network. Enterasys NAC can be leveraged to provide information to SIM solutions, by mapping an IP address to an identity, such as a MAC address or username and location, for a more complete representation of the attack source or target on the network. In this way, the Enterasys NAC solution further enhances the operation of existing security technologies deployed on the network.

Required and Optional Components

This section summarizes the required and optional components for Model 1.

Table 2-1 Component Requirements for Detection and Tracking

Component	Detection and Tracking
NAC Appliance	Required
NetSight NAC Manager	Required
NetSight Console	Required
Assessment	*Optional*
RADIUS Server	*Optional*
NetSight Policy Manager	*Optional*
NetSight Inventory Manager	*Optional*

The NAC Gateway and NAC Controller are the NAC appliances used to implement the out-of-band and inline network access control functionality on the network.

NetSight NAC Manager is the software application used to centrally manage the NAC appliances deployed on the network.

NetSight Console is the software application used to monitor the health and status of infrastructure devices in the network, including switches, routers, and Enterasys NAC appliances (NAC Gateways and NAC Controllers).

Assessment functionality is optional because in this deployment model, end-systems are not being assessed for security posture compliance when connecting to the network.

A RADIUS server is only required if out-of-band network access control using the NAC Gateway, or inline network access control using the Layer 2 NAC Controller, is implemented with web-based and/or 802.1X authentication.

NetSight Policy Manager is not required because additional policies and authorization levels do not need to be defined for this deployment model.

NetSight Inventory Manager is an optional component, providing comprehensive network inventory and change management capabilities.

Model 2: End-System Authorization

This NAC deployment model implements the detection, authentication, and authorization of connecting end-systems, to control access to network resources based on user and end-system identity, as well as location. In Model 1, end-systems and end users are detected and tracked on the network over time. This gives IT operations visibility into what devices are connected to the network, who is using these devices, and where these devices are connected. In model 2, the device identity, user identity, and/or location information is used to authorize the connecting end-system with a certain level of network access. It is important to note that in this model, network access is not being controlled based on end-system assessment results. Assessment will be introduced in the next NAC deployment model.

Implementation

In Model 2, end-systems can be detected, authenticated, and authorized in different ways depending on whether inline or out-of-band network access control is implemented.

Out-of-Band NAC

For out-of-band NAC utilizing the NAC Gateway, NAC functions are implemented in the following way:

Detection - End-systems are detected via the receipt of RADIUS packets from an access edge switch attempting to authenticate an end-system.

Authentication - If the end-system is 802.1X or web authenticating to the network, the NAC Gateway proxies the RADIUS authentication request to a backend authentication (RADIUS) server to validate the identity of the user/device connecting to the network. For end-systems that are MAC authenticating to the network, the NAC Gateway can be configured to either proxy the MAC authentication requests to a RADIUS server or locally authorize MAC authentication requests at the NAC Gateway. If only MAC authentication is deployed on the network and the NAC Gateway is configured to locally authorize MAC authentication requests, then a backend RADIUS server is not required for the Enterasys NAC solution.

Authorization - The NAC Gateway allocates the appropriate network resources to the end-system based on device identity, user identity, and location. For Enterasys policy-enabled edge switches, the NAC Gateway formats information in the RADIUS authentication messages that directs the edge switch to dynamically assign a particular policy to the connecting end-system. For RFC 3580-capable edge switches, the NAC Gateway formats information in the RADIUS authentication messages (in the form of RFC 3580 VLAN Tunnel attributes) that directs the edge switch to dynamically assign a particular VLAN to the connecting end-system. The NAC Gateway may deny the end-system access to the network by sending a RADIUS Access-Reject message to the edge switch or assign the end-system a set of network resources by specifying a particular policy or VLAN to assign to the authenticated end-system on the edge switch.

Inline NAC

For inline NAC utilizing the Layer 2 or Layer 3 NAC Controller, NAC functions are implemented in the following way:

Detection - End-systems are detected via the receipt of RADIUS packets from an access edge switch attempting to authenticate an end-system.

Authentication - One of two authentication configurations can be implemented on the NAC Controller. Authentication can be disabled altogether, trusting that the downstream infrastructure devices authenticated the end-system and permitted network access. Alternately, MAC registration can be implemented for new devices connecting to the network, where a username and password and/or a sponsor username and password must be validated against a backend LDAP-compliant database before network access is permitted.

Authorization - The NAC Controller allocates the appropriate network resources to the end-system by assigning a policy locally on the controller to the traffic sourced from the end-system.

The NAC Controller may either deny the end-system access to the network or assign the end-system to a particular set of network resources by specifying a particular policy.

Features and Value

In addition to the features and values found in Model 1, the following are key pieces of functionality and value propositions supported by Model 2, End-System Authorization:

Location-Based Authorization

In addition to providing visibility into who, what, when, and where devices and users are connecting to the network, this deployment model allows IT operations to control access to the network with different levels of authorization based on these parameters. For location-based authorization, the Enterasys NAC solution can assign a level of access to a connecting end user or device based on which area of the network the end-system is connected, through the configuration of Security Domains. For example, when an engineer connects to the network from a controlled area of the network such as the lab, or a faculty member connects to the network from a physically secured faculty office, the engineer and faculty member are appropriately authorized to access sensitive information residing on internal servers. However, if the same users connect to the network from an unsecured area of the network such as the open wireless LAN available in the enterprise's lobby or campus, or in a student dormitory, then these end-systems can be authorized with a different level of network access, possibly restricting communication to the internal servers and other resources on the network.

Furthermore, the NAC solution can also lock a device to a specific switch or switch port, using the “Lock MAC” feature. If the device is moved to any other switch port on the network, it will not be able to connect. For example, a printer or a server containing sensitive data may be connected to the network at a specific location, such as behind a firewall or on a particular VLAN for security reasons. Physically moving the connection of these devices to an open area of the network increases the risk of these devices being attacked and compromised because they would no longer be protected by the security mechanisms that were put in place on the network. The “Lock MAC” feature can be used to limit the mobility of specific devices and avoid malicious or unintentional misconfigurations on the network, thereby reducing risk.

Device-Based Authorization

With this NAC deployment model, end-systems are authorized with access to a specific set of network resources based on the end-system's MAC address. For initial implementation, the Enterasys NAC solution is configured in a mode where all MAC addresses of connecting end-systems are permitted onto the network and dynamically learned. The Enterasys NAC solution is then configured to allow only known MAC addresses onto the network, assigning each end-system a particular authorization level. Any new MAC address connecting to the network is assigned a different authorization level, such as denied access, restricted access, or allowed access if the user is able to properly register their device to the network.

The Enterasys NAC solution is able to authorize specific devices or classes of devices (based on MAC address OUI prefix) with access to a specific set of network resources through the configuration of MAC overrides. For example, an end-system that is known to be infected with a worm, a publicly accessible machine, or a machine belonging to guest user may be authorized with a restrictive set of network resources or completely denied network access, regardless of where and when this device connects. In contrast, an end-system belonging to the IT operations group may be permitted unrestricted access to network resources for infrastructure troubleshooting and maintenance purposes, regardless of where and when the device connects to the network. If you add location-based authorization (as discussed above) to this example, then unrestricted access for end-systems belonging to the IT operations group is only provisioned by the Enterasys NAC solution when the devices connect to switches in the Network Operations Center (NOC). This level of granularity in provisioning access to connecting devices protects against possible MAC spoofing attacks.

In addition to authorizing a particular device with a set of network resources, groups of devices such as IP phones, printers, and workstations can be provisioned a specific set of network resources using MAC address OUI prefix or custom MAC address mask. For example, IP phones may be identified by the Polycom MAC address OUI prefix 00:04:F2:XX:XX:XX and assigned the Voice VLAN and a high QoS.

In summary, device-based authorization supports the provisioning of network resources to a connecting end-system based on the device's identity as well as location. This provides the ability to restrict end-systems that pose a threat to the network, provide special access to particular devices, and provision end-systems or sets of end-systems with access to required sets of network resources to ensure business continuity.

User-Based Authorization

With this NAC deployment model, end-systems can be authorized with access to a specific set of network resources based on the user logged into the end-system and their organizational role within the enterprise. For example, a user who is an engineer may be allocated prioritized access to the engineering servers deployed on the network while being denied access to servers utilized by the HR or legal departments. Furthermore, a user who is known to be launching malicious attacks against critical resources on the network or was terminated from a position within the company may be authorized a restrictive set of network resources or outright denied network access, regardless of where and when this user connects to the network. In contrast, a user in the IT operations group or a technician sent to repair a device on the network may be permitted unrestricted access to network resources for troubleshooting and maintenance purposes, regardless of where and when the user connects to the network, or only from inside the NOC.

In summary, user-based authorization supports the provisioning of network resources to connecting users based on the user's identity and successful authentication, as well as their location on the network, affording such capabilities as denying users that pose a threat to the network, providing particular employees with special access, and provisioning users in general with appropriate access to the required sets of network resources, to ensure business continuity.

MAC Registration

Enterasys NAC provides support for MAC Registration, also known as Network or Guest Registration. This solution forces any new end-system connected on the network to provide the user's identity in a web page form before being allowed access to the network, without requiring the intervention of IT operations. This means that end users are automatically provisioned network access on demand without time-consuming and costly help desk requests or network infrastructure reconfigurations.

In addition, IT operations has visibility into the end-systems and their registered users on the network (for example, guests, students, contractors, and employees) without requiring the deployment of backend authentication and directory services to manage these users. This binding between user identity and machine is useful for auditing, compliance, accounting, and forensics purposes on the network.

Furthermore, MAC Registration supports a functionality referred to as “sponsored registration” requiring that end users are only allowed to register to the network when accompanied by a trusted sponsor; an internal user to the organization with valid credentials. When an end user is registering to the network, a sponsor must enter a username and possibly a password in the registration web page. This sponsor username and password can be validated against an existing database on the network to authenticate the sponsor's identity. Sponsors may be allowed to securely access an administrative web page where they can delete, add, and modify registered end-systems on the network that they have sponsored. With sponsored registration enabled, IT operations can hold trusted users accountable for guests brought on the enterprise network, while controlling access for only appropriate guests.

Post-Connect NAC integration with NetSight Automated Security Manager

NetSight Automated Security Manager (ASM), a software application that is part of the NetSight Suite, has the capability to search the infrastructure and locate the switch port of connection, based on the receipt of a security event for a particular IP address. ASM responds to this event by disabling the port or assigning a VLAN (such as the quarantine VLAN) to the port. In response to a real-time security threat detected on the network, ASM can be configured to notify NAC Manager on this event, dynamically quarantining the MAC address. This effectively restricts the quarantined end-system from accessing the network from any location, enterprise-wide. If ASM reverses the quarantine action, it notifies NAC Manager, and the quarantine is automatically removed and the end-system is dynamically re-admitted access to network resources. Therefore, the deployment of Enterasys NAC further increases the security posture of the network by integrating with the reactive threat response capabilities of ASM, in addition to controlling access and authorizing connecting devices.

Required and Optional Components

This section summarizes the required and optional components for Model 2.

Table 2-2 Component Requirements for Authorization

Component	Authorization
NAC Appliance	Required
NetSight NAC Manager	Required
NetSight Console	Required
Assessment	*Optional*
RADIUS Server	*Optional*
NetSight Policy Manager	*Optional*
NetSight Inventory Manager	*Optional*

The NAC Gateway and NAC Controller are the NAC appliances used to implement the out-of-band and inline network access control functionality on the network.

NetSight NAC Manager is the software application used to centrally manage the NAC appliances deployed on the network.

NetSight Console is the software application used to monitor the health and status of infrastructure devices in the network, including switches, routers, and Enterasys NAC appliances (NAC Gateways and NAC Controllers).

Assessment functionality is optional because in this deployment model, end-systems are not being assessed for security posture compliance when connecting to the network.

A RADIUS server is only required if out-of-band network access control using the NAC Gateway, or inline network access control using the Layer 2 NAC Controller, is implemented with web-based and/or 802.1X authentication.

NetSight Policy Manager is required for all inline NAC deployments, and recommended for out-of-band NAC deployments that utilize Enterasys policy-capable switches. Policy Manager provides the ability to centrally define and configure the authorization levels or policies.

NetSight Inventory Manager is an optional component, providing comprehensive network inventory and change management capabilities.

Model 3: End-System Authorization with Assessment

This NAC deployment model implements the detection, authentication, assessment and authorization NAC functionalities for connecting end-systems. In Model 2, end-systems and end users connected to the network are authorized based on the device identity, user identity, and/or location information. Model 3 extends the authorization decision in NAC to one additional dimension — the security posture of the end-system as determined from an assessment. The assessment can be executed through agent-based or agent-less techniques and can identify different pieces of information about the device, such an antivirus software configuration, operating system patches installed, software applications installed and running, processes running, services configured, and registry values set.

It is important to note that it is not necessary to configure the Enterasys NAC solution to quarantine end-systems that fail assessment. In fact, during the initial rollout of NAC on the enterprise network, it is highly recommended that end-systems are not restricted access to the network in any way before, during, or after failed assessment. This passive NAC configuration allows the IT administrator to baseline the configuration of devices on the network and understand the current landscape of its assets without impacting network connectivity for connecting end-systems. In this configuration, it is not necessary to inform the end users that they are being assessed or have failed assessment because there is little-to-no impact on network connectivity during this assessment. End-systems can be scanned in the background providing the network administrator with important visibility into how devices are configured on their network, while end users can utilize the network as desired. Then, when the network administrator is ready, the Enterasys NAC solution can be configured with the click of a button to immediately restrict access for end-systems that have failed assessment.

Implementation

In Model 3, end-systems can be detected and tracked, authenticated, assessed, and authorized in different ways depending on whether inline or out-of-band network access control is implemented in the Enterasys NAC solution.

Out-of-Band NAC

For out-of-band Enterasys NAC deployments utilizing the NAC Gateway, NAC functions are implemented in the following way:

Detection - As described in Model 2.

Authentication - As described in Model 2.

Assessment - The NAC Gateway can leverage either local assessment services and/or remote assessment services deployed on the network. The NAC Gateway's local assessment services include agent-less assessment which can execute various server-side checks (whether an FTP server is running or if the HTTP server is out-of-date) and client-side checks (running applications, software configurations, installed operating system patches) provided end-system administrative credentials are available for remote login to connecting devices. Additionally, the NAC Gateway's local assessment services also include agent-based assessment using a Java Web Start-based client application that allows execution of server-side and client-side checks without requiring administrative credentials or special host firewall configurations.

The NAC Gateway's remote assessment services include agent-less and agent-based assessment on other NAC Gateways deployed on the network and/or third-party vulnerability scanners such as Nessus and Lockdown Enforcer. As end-systems connect to the network, assessments can be load-balanced among all of the configured assessment services or a defined pool. This provides maximum scalability and flexibility, and minimizes the amount of time necessary to complete an end-system assessment.

Authorization - The NAC Gateway allocates the appropriate network resources to the end-system based on authentication, location, and/or assessment results. For Enterasys policy-enabled edge switches, the NAC Gateway formats information in the RADIUS authentication messages that directs the edge switch to dynamically assign a particular policy to the connecting end-system. For RFC 3580-capable edge switches, the NAC Gateway formats information in the RADIUS authentication messages in the form of RFC 3580 VLAN Tunnel attributes that directs the edge switch to dynamically assign a particular VLAN to the connecting end-system. If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC Gateway can either deny the end-system access to the network by sending a RADIUS access reject message to the edge switch or quarantine the end-system with a highly restrictive set of network resources (or possibly permit network access) by specifying a particular policy or VLAN to assign to the authenticated end-system on the edge switch.

Inline NAC

For inline Enterasys NAC deployments utilizing the Layer 2 or Layer 3 NAC Controller, the NAC functions are implemented in the following way:

Detection - As described in Model 2.

Authentication - As described in Model 2.

Assessment - The NAC Controller can leverage either local assessment services and/or remote assessment services deployed on the network, as previously described for the NAC Gateway. The NAC Controller's local assessment services include agent-less assessment which can execute various server-side checks and client-side checks. Local assessment services also include agent-based assessment using a Java Web Start-based client application that allows execution of server-side and client-side checks. The NAC Controller's remote assessment services include agent-less and agent-based assessment with NAC Gateways and/or third-party vulnerability scanners such as Nessus and Lockdown Enforcer. As end-systems connect to the network, assessment can be load-balanced among all of the configured assessment services to provide maximum scalability and flexibility while minimizing assessment times.

Authorization - The NAC Controller allocates the appropriate network resources to the end-system based on authentication and/or assessment results. This is implemented by assigning a policy to traffic sourced from the end-system locally on the controller. If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC Controller can either deny the end-system access to the network, quarantine the end-system with a highly restrictive set of network resources, or permit network access by specifying a particular policy.

Features and Value

In addition to the features and values found in Model 1 and Model 2, the following are key pieces of functionality and value propositions supported by Model 3, End-System Authorization with Assessment:

Extensive Security Posture Compliance Verification

The following describes a few examples of tests that can be executed for connecting end-systems and the relevance of these tests from a compliance and security standpoint:

- Antivirus software configuration

  The NAC solution can determine if an end-system has antivirus software installed, if it is properly configured (real-time protection is enabled), if it is up-to-date with the most recent virus definition file, and if it is enabled. Antivirus software has the ability to detect infections as they happen, and to prevent further propagation of the virus to other end-systems. It is important to verify that end-systems are protected with antivirus software when they connect to the network, in case the end-system is subsequently infected with a worm or virus after connectivity is established.

- Operating system patch level

  The NAC solution can determine if the end-system is up-to-date with the latest operating system patches. This ensures that any vulnerabilities present in services running on unpatched laptops are appropriately remediated, so that attacks that target those vulnerabilities are not successful, if they reach the device on the network.

- Malware infection

  The NAC solution can determine if the end-system is infected with malware (worms, viruses, spyware, and adware) by identifying backdoor ports on which the end-system is listening, running processes and services, and/or registry key settings. By identifying infected end-systems prior to network connection, the NAC solution protects other end-systems on the network from possible infection and prevents the unnecessary consumption of network bandwidth.

- Host firewall configuration

  The NAC solution can determine if the end-system has a host firewall enabled. By having a firewall enabled, the end-system can protect itself against attacks targeting vulnerable services and applications on the device.

- Peer-to-Peer (P2P) file sharing software configuration

  The NAC solution can determine if the end-system is installed with or is running a P2P file sharing application. Since P2P file sharing applications facilitate the illegal file transfer of copyrighted data on the network and can be used for recreational purposes, it is important that the NAC solution validates that this type of application is not in use on end-systems prior to network connection. This avoids legal issues involved with the transfer of copyrighted data or loss of productivity due to inappropriate online activity.

- Application configuration

  The NAC solution can determine which services and applications are installed and enabled on the end-system. Certain applications should be removed from the device prior to establishing connectivity because they may have a negative impact on the operation of the end-system, distract the end user from business functions, or be used to launch attacks on the network. Furthermore, particular services may be outdated and vulnerable to attack. These services should either be updated or disabled to minimize the risk to connecting end-systems on the network. The NAC solution facilitates this reconfiguration of applications on an end-system prior to network connection, to ensure maximum security and productivity when the device connects.

Diverse Security Posture Compliance Verification

In order for a NAC solution to be effective, inclusion of **all** end-systems in the network environment must be addressed when detecting, authenticating, assessing, and authorizing devices. The Enterasys NAC solution supports a diverse end-system environment, and provides integrated security and management regardless of what type of devices are connected to the business network.

Enterasys leverages two assessment models: agent-based and agent-less. An agent-based assessment and an agent-less assessment are both critical to ensuring that any end-system of any type can be included in the NAC process. There are several reasons why both assessment models are critical to a complete NAC solution. Security agents loaded onto managed end-systems offer extensive assessment capabilities. If an agent is required, a new end-system connecting to the network that has not downloaded the agent can be quarantined and redirected to a web page. The web page provides information on how the agent can be downloaded and installed on the end-system to begin its assessment.

However, there are types of end-systems in a typical network that may not be able to load a software agent, such as IP phones, security cameras, or printers. If a security agent is not available for a device (or the operating systems running the device), an agent-less approach is the only way to assess the end-system. In addition, consider end-systems that could normally hold an agent, but are not under the control of the IT organization. In the case of guest networking that provides support for contractors, vendors, and the public, the desire may be to support minimal or specific network services, but still ensure the safety and security of the network and the people using it. It is not enough to simply use a network usage policy to restrict the services a guest user is allowed to access. Because the guest is leveraging the same network infrastructure as the critical business users, it is important that proactive security measures are applied to the guest just as they are to a managed user. This is another case where an agent-less approach to end-system assessment can be critical to ensuring a comprehensive NAC strategy.

Both the agent-based and the agent-less assessment models can be deployed and integrated together in the Enterasys NAC solution.

Required and Optional Components

This section summarizes the required and optional components for Model 3.

Table 2-3 Component Requirements for Authorization with Assessment

Component	Authorization with Assessment
NAC Appliance	Required
NetSight NAC Manager	Required
NetSight Console	Required
Assessment Service	Required
RADIUS Server	*Optional*
NetSight Policy Manager	*Optional*
NetSight Inventory Manager	*Optional*

The NAC Gateway and NAC Controller are the NAC appliances used to implement the out-of-band and inline network access control functionality on the network.

NetSight NAC Manager is the software application used to centrally manage the NAC appliances deployed on the network.

NetSight Console is the software application used to monitor the health and status of infrastructure devices in the network, including switches, routers, and Enterasys NAC appliances (NAC Gateways and NAC Controllers).

Assessment functionality is required because in this deployment model, connecting end-systems are being assessed for security posture compliance.

A RADIUS server is only required if out-of-band network access control via the NAC Gateway is implemented with web-based and/or 802.1X authentication.

NetSight Policy Manager is required for all inline NAC deployments, and recommended for out-of-band NAC deployments that utilize Enterasys policy-capable switches. Policy Manager provides the ability to centrally define and configure the authorization levels or policies.

NetSight Inventory Manager is an optional component, providing comprehensive network inventory and change management capabilities.

Model 4: End-System Authorization with Assessment and Remediation

This NAC deployment model implements all five NAC functions: detection, authentication, assessment, authorization, and remediation. In Model 3, end-systems and end users connected to the network are authorized based on the device identity, user identity, location, and/or security posture information. And, as explained in Model 3, it was not necessary to quarantine noncompliant end-systems while phasing in the NAC solution on the network. However, once a restrictive authorization level is allocated to noncompliant end-systems, it is important to inform the end user of the restrictions and provide the steps they can execute for self-repair of the device. This is the process of assisted remediation, which is the NAC function introduced in Model 4.

Assisted remediation informs end users when their end-systems have been quarantined due to network security policy non-compliance, and allows end users to safely remediate their non-compliant end-systems without assistance from IT operations. The process takes place when an end-system connects to the network and assessment is performed. End users whose systems fail assessment are notified via web redirection that their systems have been quarantined, and are instructed in how to perform self-service remediation specific to the detected compliance violations.

Once the remediation steps have been successfully performed and the end-system is compliant, the end user can initiate an on-demand reassessment of the end-system and can be allocated the appropriate network resources, again without the intervention of IT operations.

Implementation

In Model 4, end-systems can be detected, authenticated, assessed, authorized, and remediated in different ways depending on the whether inline or out-of-band network access control is implemented in the Enterasys NAC solution.

Out-of-Band NAC

For out-of-band Enterasys NAC deployments utilizing the NAC Gateway, NAC functions are implemented in the following way:

Detection - As described in Model 2.

Authentication - As described in Model 2.

Assessment - As described in Model 3.

Authorization - As described in Model 3.

Remediation - When end-systems are quarantined by the NAC Gateway, the network must be configured to direct all traffic from the quarantined end-systems to the NAC Gateway. This can be implemented by configuring policy-based routing on a router inline with the traffic sourced from quarantined end-systems. This router would be configured to send all web traffic from quarantined end-systems to the NAC Gateway, which then serves back the remediation web page to the end user.

The way the router identifies the traffic from quarantined end-systems differs between a network composed of policy-enabled switches in the access edge or a network composed of switches implementing RFC 3580 dynamic VLAN assignment in the access edge. For an Enterasys policy-enabled edge, the Quarantine policy can be configured to rewrite the Type of Service (ToS) value of HTTP traffic to a particular setting that matches the policy-based routing configuration. For an RFC 3580 capable edge, the policy-based routing would be configured to match the source IP address of the HTTP traffic being generated from the subnets that corresponds to the Quarantine and/or Assessing VLAN. In either case, by directing the HTTP traffic from quarantined end-systems over to the NAC Gateway, the NAC Gateway will serve back the remediation web page to the noncompliant end-system.

Inline NAC

For inline Enterasys NAC deployments utilizing the Layer 2 or Layer 3 NAC Controller, the NAC functions are implemented in the following way:

Detection - As described in Model 2.

Authentication - As described in Model 2.

Assessment - As described in Model 3.

Authorization - As described in Model 3.

Remediation - When an end-system is quarantined by the NAC Controller, all web traffic sourced from the quarantined end-system is redirected to the local Remediation Web Service running on the NAC Controller. The NAC Controller then returns the remediation web page to the noncompliant end-system. No additional configurations are required on the network because the NAC Controller exists inline with the traffic from quarantined end-systems.

Features and Value

In addition to the features and values found in Model 1, Model 2, and Model 3, the following are key pieces of functionality and value propositions supported by Model 4, End-System Authorization with Assessment and Remediation:

Self-Service Remediation

If a user's PC is suddenly quarantined and the user is not able to access the expected types of services, it is not only important that information of this event is available to IT, but also that the user is directly notified of the cause of service disruption. If they are not notified about the quarantine action, the user will likely believe that there is a network communication problem. Implementing a NAC solution that can quarantine users without notification, may inadvertently increase calls to the IT help desk from users who are not able to access needed services.

With the Enterasys NAC solution, network-based notification and remediation are integrated. Once an end-system is put into a quarantine state, notification is achieved by redirecting the non-compliant end-system's web traffic to a remediation web page. The web page can be maintained by the IT organization and can include details about why the end-system has been quarantined and how a user can fix issues that are causing the non-compliant state. The layout and information presented on this web page is fully customizable including changing header and footer information, altering information presented to the user, and controlling the amount of time or the number of times an end-system is allowed to initiate reassessment after attempting remediation.

Although the end-system may be able to access the network and the remediation web page, communication is provisioned through a set of policy rules to ensure that there is no danger to the rest of the network. In order for a quarantined user to regain access to network services, they must first remediate the problem that actually caused the quarantine to occur in the first place. However, remediation does not always have to be made available to the user. Consider the situation where a user is acting maliciously and threatening the network and its services. Remediation may not be desirable, and instead a persistent quarantine policy may be enforced to keep the user from causing any harm.

The key to this process is the ability of the network to enforce a usage policy that completely protects all critical resources and other users, but allows access to key remediation assets such as web servers with security patches. The Enterasys NAC solution allows a quarantine policy to be established with a very specific set of policy rules that can filter and control network traffic with specific source and destination characteristics as well as specific application identifiers (UDP/TCP ports). In addition, the Enterasys NAC solution will support an unlimited number of different quarantine policy roles, which means that the solution can support varying degrees of network usage restrictions depending upon the severity of the non-compliance or security breach. This is different from many other NAC solutions that only offer a VLAN "parking lot" for end-systems that need to be quarantined.

Required and Optional Components

This section summarizes the required and optional components for Model 4.

Table 2-4 Component Requirements for Authorization with Assessment and Remediation

Component	Authorization with Assessment and Remediation
NAC Appliance	Required
NetSight NAC Manager	Required
NetSight Console	Required
Assessment Service	Required
RADIUS Server	*Optional*
NetSight Policy Manager	*Optional*
NetSight Inventory Manager	*Optional*

The NAC Gateway and NAC Controller are the NAC appliances used to implement the out-of-band and inline network access control functionality on the network.

NetSight NAC Manager is the software application used to centrally manage the NAC appliances deployed on the network.

NetSight Console is the software application used to monitor the health and status of infrastructure devices in the network, including switches, routers, and Enterasys NAC appliances (NAC Gateways and NAC Controllers).

Assessment functionality is required because in this deployment model, connecting end-systems are being assessed for security posture compliance.

A RADIUS server is only required if out-of-band network access control via the NAC Gateway is implemented with web-based and/or 802.1X authentication.

NetSight Policy Manager is required for all inline NAC deployments, and recommended for out-of-band NAC deployments that utilize Enterasys policy-capable switches. Policy Manager provides the ability to centrally define and configure the authorization levels or policies.

NetSight Inventory Manager is an optional component, providing comprehensive network inventory and change management capabilities.

Summary

Enterasys supports all of the five key NAC functions: detection, authentication, assessment, authorization, and remediation. However, not all five functions need to be implemented concurrently in a NAC deployment to derive value from the solution. The four NAC deployment models each yield unique value propositions to the IT personnel managing the network, and provide a logical progression to deploying the full Enterasys NAC solution.

The following table summarizes the value and features of each deployment model.

Table 2-5 Enterasys NAC Deployment Models

Deployment Model	Value
Model 1: End-System Detection and Tracking	• End-system and user tracking. • IP-to-ID functionality for Security Information Management (SIM).
Model 2: End-System Authorization	In addition to the values from Model 1: • Location-based authorization using Security Domains and “Lock MAC” features. • Special handling of end-systems or users with MAC/User overrides that let you specify a unique set of authentication and authorization parameters for particular devices or users. • MAC registration where new end-systems register via a web page before being allowed access to the network. • Location-independent end-system quarantine action with NetSight Automated Security Manager integration.
Model 3: End-System Authorization with Assessment	In addition to the values from Models 1 and 2: • Security posture compliance verification of connecting end-systems with dynamic quarantine action using integrated or external assessment.
Model 4: End-System Authorization with Assessment and Remediation	In addition to the values from Models 1, 2, and 3: • Self-service remediation of non-compliant end-systems without impacting IT operations.

3

Use Scenarios

This chapter describes four NAC use scenarios that illustrate how the type of NAC deployment is directly dependent on the infrastructure devices deployed in the network. For some network topologies, inline network access control utilizing the NAC Controller may be required while for other network configurations, the NAC Gateway implementing out-of-band NAC may be used.

The Enterasys NAC solution is capable of implementing network access control for all four use scenarios as well as environments with mixed use scenarios that may require the concurrent deployment of the NAC Gateway and the NAC Controller. Regardless of the scenario that is deployed, all NAC Gateways and NAC Controllers are centrally managed by the NetSight NAC Manager software application.

For the intelligent wired access edge and intelligent wireless access edge use scenarios, the term “intelligent” refers to a network topology where the access edge is composed of Enterasys policy-enabled switches capable of supporting authentication and policy enforcement, or third-party switches capable of supporting authentication and dynamic VLAN assignment as defined in RFC 3580.

Scenario 1: Intelligent Wired Access Edge

In the intelligent wired access edge use scenario, the edge switches that compose the network access layer are capable of providing authentication (802.1X, web-based, or MAC) for connecting end-systems, and they are also capable of being an authorization point for these end-systems through Enterasys policy and/or dynamic VLAN assignment as specified in RFC 3580.

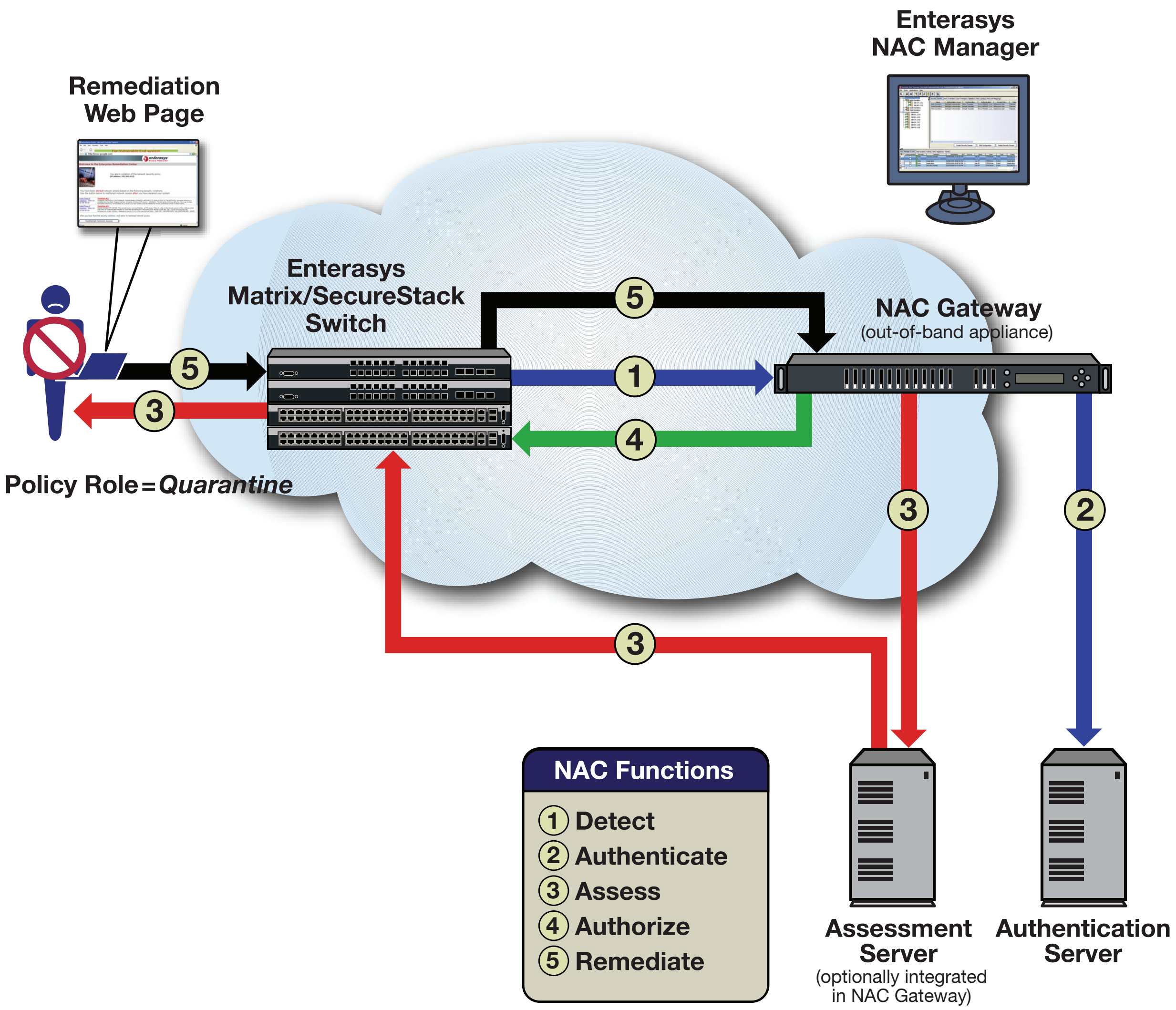
For this use scenario, the NAC Gateway appliance is deployed for out-of-band network access control, leveraging the intelligent infrastructure devices in the access edge as the authorization point for connecting end-systems.

It is important to note that Enterasys policy-enabled switches provide increased security over third-party switches that support RFC 3580. By using port-level granular traffic control, users quarantined with Enterasys policy can be restricted from communicating with other quarantined users, even if co-located on the same VLAN. In a Quarantine VLAN as implemented on third-party RFC 3580 capable switches, a quarantined user poses a threat to other quarantined users within the same Quarantine VLAN because the authorization point is usually implemented at the exit point of the VLAN via Access Control Lists (ACLs).

Policy-Enabled Edge

The following figure illustrates how the NAC Gateway and the other Enterasys NAC components work together in a network with policy-enabled edge switches to provide a comprehensive NAC solution.

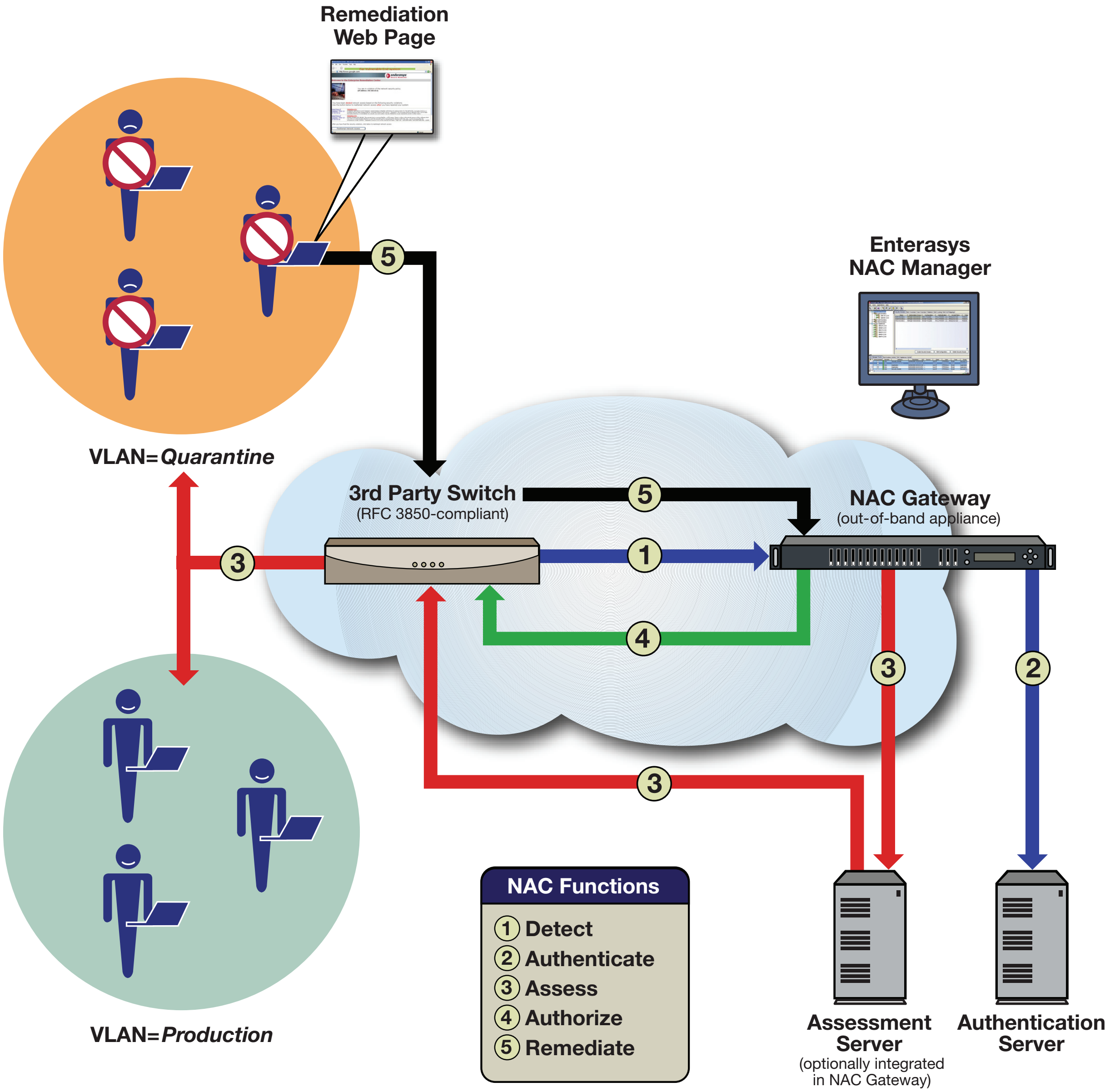
Figure 3-1 Intelligent Wired Access Edge with Enterasys Policy-Enabled Devices



RFC 3580 Capable Edge

In this figure the NAC Gateway and the other Enterasys NAC components provide network access control for a network with third-party switches that support RFC 3580.

Figure 3-2 Intelligent Wired Access Edge with RFC 3580 Capable Devices



Scenario 1 Implementation

In the intelligent wired edge use scenario, the five NAC functions are implemented in the following manner:

1. Detection - The user's end-system connects to the network. The edge switch sends a RADIUS authentication request (802.1X, web-based, or MAC authentication) with the associated credentials to the NAC Gateway.

2. Authentication - If the end-system is authenticating to the network using 802.1X or web-based authentication, the NAC Gateway proxies the RADIUS authentication request to a backend authentication (RADIUS) server to validate the identity of the end user/device. For end-systems that are MAC authenticating to the network, the NAC Gateway can be configured to either proxy the MAC authentication requests to the RADIUS server or locally authorize MAC authentication requests. If only MAC authentication is deployed on the network, and the NAC Gateway is configured to locally authorize MAC authentication requests, a backend RADIUS server is not required for the Enterasys NAC solution.

3. Assessment - After the identity of the end-system or end user is validated via authentication, the NAC Gateway requests an assessment of the end-system according to predefined security policy parameters. The assessment can be agent-based or agent-less, and is executed locally by the NAC Gateway's assessment functionality and/or remotely by a pool of assessment servers.

4. Authorization - Once authentication and assessment are complete, the NAC Gateway allocates the appropriate network resources to the end-system based on authentication and/or assessment results. For Enterasys policy-enabled edge switches, the NAC Gateway formats information in the RADIUS authentication messages that directs the edge switch to dynamically assign a particular policy to the connecting end-system. For RFC 3580-capable edge switches, the NAC Gateway formats information in the RADIUS authentication messages (in the form of RFC 3580 VLAN Tunnel attributes) that directs the edge switch to dynamically assign a particular VLAN to the connecting end-system. If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC Gateway can either deny the end-system access to the network by sending a RADIUS access reject message to the edge switch, or quarantine the end-system by assigning a Quarantine policy or VLAN to the end-system on the edge switch.

5. Remediation - When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that describes the compliance violations and provides remediations steps for the user to execute in order to achieve compliance. After taking the appropriate remediation steps, the end user clicks on a button on the web page to reattempt network access, forcing the re-assessment of the end-system. At this point, the Enterasys NAC solution transitions the end-system through the entire NAC cycle of detection, authentication, assessment, and authorization, re-assessing the security posture of the end-system to determine if the remediation steps were successfully followed. If the end-system is now compliant with network security policy, the NAC Gateway authorizes the end-system with the appropriate policy or VLAN. If the end-system is not compliant, the end-system is restricted access to the network and the process starts again.

It is important to note that if the wired edge of the network is non-intelligent (unmanaged switches and hubs) and is not capable of authenticating and authorizing locally connected end-systems, it is possible to augment the network topology to allow implementation of out-of-band NAC with the NAC Gateway. This can be accomplished without replacing the physical edge of the network, by adding an intelligent edge switch that possesses specialized authentication and authorization features.

The Enterasys Matrix N-series switch is capable of authenticating and authorizing numerous end-systems connected on a single port through its Multi-User Authentication (MUA) functionality and may be positioned upstream from non-intelligent third-party edge devices to act as the intelligent edge on the network. The Matrix N-series switch is capable of authenticating and authorizing multiple devices connected to a single port for a variety of network topologies, ranging from an IP phone cascaded with a PC on a single Matrix N-series port, to a stack of non-intelligent edge switches uplinked to a single Matrix N-series port where over 1000 end-systems connect. In this configuration, the Matrix N-series acts as the intelligent edge switch on the network, although not physically located at the access edge. Each individual end-system is authenticated using 802.1X, web-based, and/or MAC authentication and is subsequently authorized on the Matrix N-series inter-switch link to the access edge. By provisioning access to network resources on the Matrix N-series using MUA, end-system traffic destined to adjacent switches on the network can be securely contained with policy at the Matrix N-series port.

Scenario 2: Intelligent Wireless Access Edge

In the intelligent wireless access edge use scenario, thick Access Points (APs) or wireless switches with thin APs provide authentication and authorization for connecting end-systems.

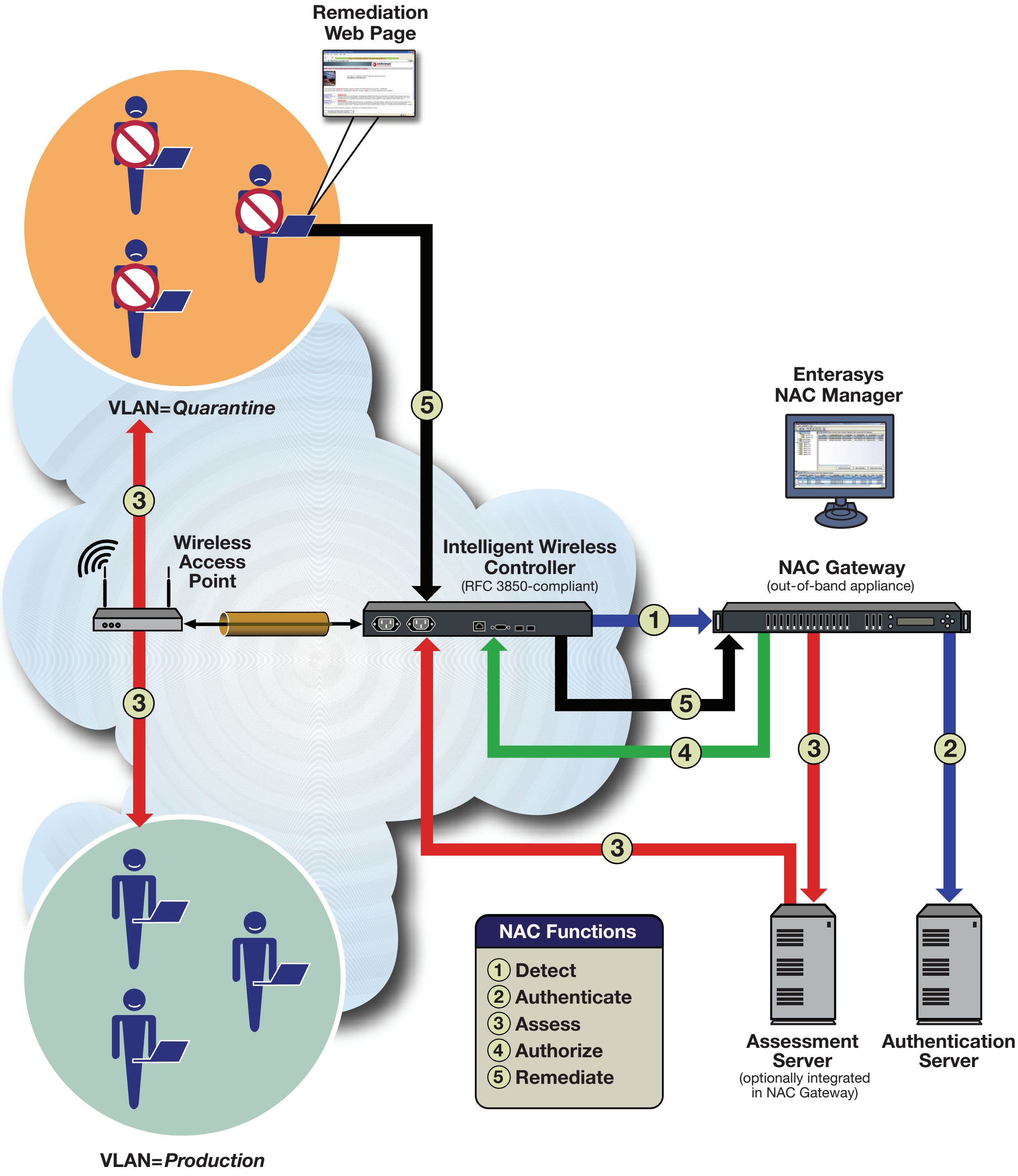
For this use scenario, the NAC Gateway appliance is deployed for out-of-band network access, leveraging the intelligent wireless infrastructure devices as the authorization point for connecting end-systems.

Thin Wireless Edge

In a thin wireless deployment, wireless switches tunnel wireless end-system traffic to and from access points deployed on the network. Most thin wireless deployments are categorized under the intelligent wireless access edge use scenario because the wireless switches are capable of providing authentication (802.1x, web-based, or MAC) and are also capable of being an authorization point either through dynamic VLAN assignment as specified in RFC 3580 or application of user-based ACLs or policy.

The following figure illustrates how the NAC Gateway and the other Enterasys NAC components work together in a thin wireless deployment.

Figure 3-3 Intelligent Wireless Access Edge - Thin APs with Wireless Switch

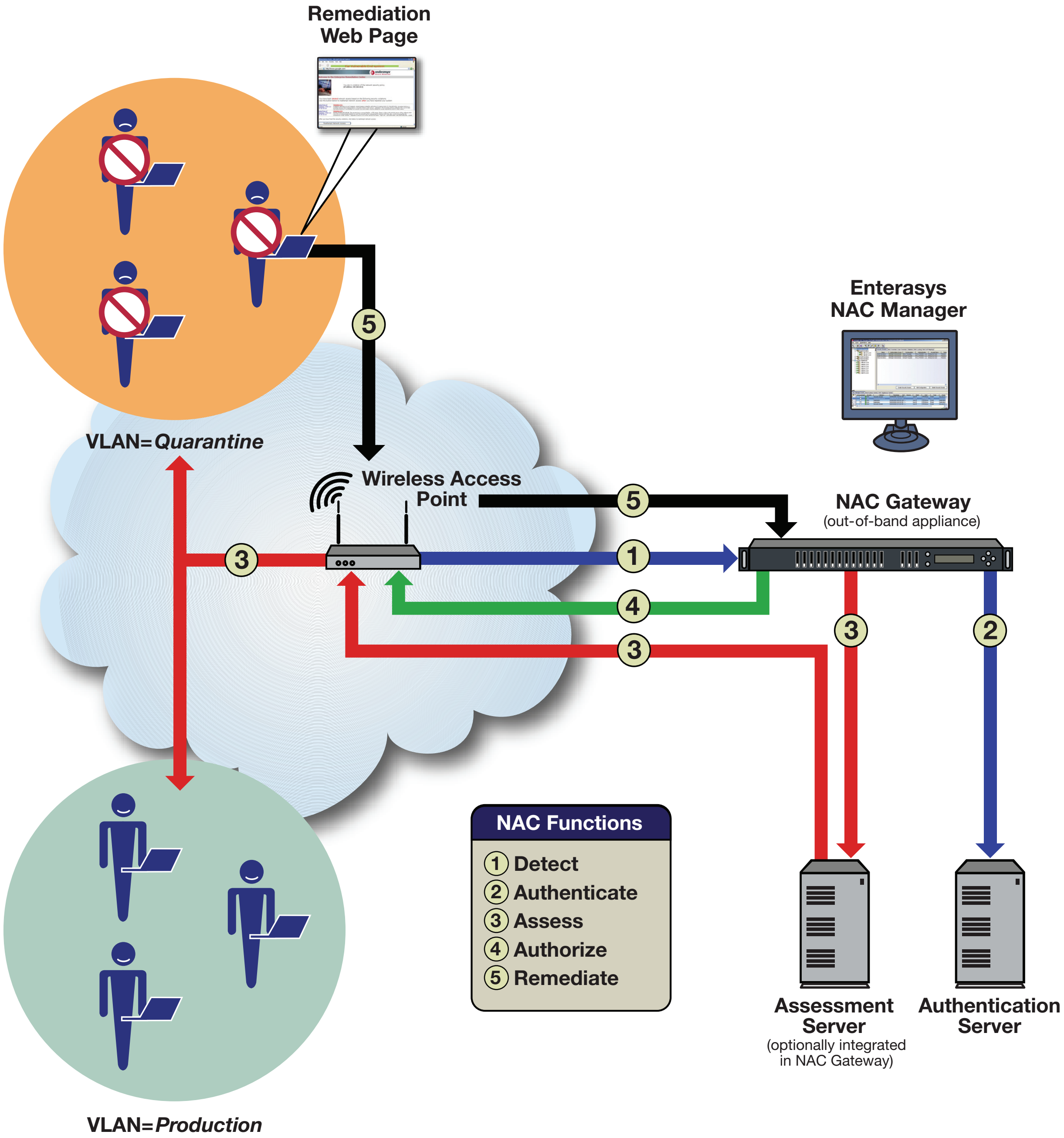


Thick Wireless Edge

In a thick wireless deployment, access points forward wireless end-system traffic directly onto the wired infrastructure without the use of a wireless switch. Thick wireless deployments may or may not be categorized under the intelligent wireless access edge use scenario depending on the functionality supported by the APs.

The following figure illustrates how the NAC Gateway and the other Enterasys NAC components provide network access control in a thick wireless deployment.

Figure 3-4 Intelligent Wireless Access Edge - Intelligent AP (RFC 3580 Compliant



Scenario 2 Implementation

In the intelligent wireless access edge use scenario, the five NAC functions are implemented in the following manner:

1. Detection - The user's end-system connects to the network. The wireless switch or thick AP sends a RADIUS authentication request (802.1X, web-based, or MAC authentication) with the associated credentials to the NAC Gateway.

2. Authentication - If the end-system is authenticating to the network using 802.1X or web-based authentication, the NAC Gateway proxies the RADIUS authentication request to a backend authentication (RADIUS) server to validate the identity of the end user/device. For end-systems that are MAC authenticating to the network, the NAC Gateway may be configured to either proxy the MAC authentication requests to the RADIUS server, or locally authorize MAC authentication requests. If only MAC authentication is deployed on the network and the NAC Gateway is configured to locally authorize MAC authentication requests, a backend RADIUS server is not required with the Enterasys NAC solution.

3. Assessment - After the identity of the end-system or end user is validated via authentication, the NAC Gateway requests an assessment of the end-system according to predefined security policy parameters. The assessment can be agent-based or agent-less, and is executed locally by the NAC Gateway's assessment functionality and/or remotely by a pool of assessment servers.

4. Authorization - Once authentication and assessment are complete, the NAC Gateway allocates the appropriate network resources to the end-system based on authentication and/or assessment results. For Enterasys policy-enabled wireless switches and access points, the NAC Gateway formats information in the RADIUS authentication messages that directs the edge switch to dynamically assign a particular policy to the wireless end-system on the wireless switch or AP, depending on the type of wireless implementation. For RFC 3580-capable wireless switches and APs, the NAC Gateway formats information in the RADIUS authentication messages (in the form of RFC 3580 VLAN Tunnel attributes) that directs the edge switch to dynamically assign a particular VLAN to the wireless end-system. If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC Gateway can either deny the end-system access to the network by sending a RADIUS access reject message, or quarantine the end-system by assigning a Quarantine policy or VLAN to the wireless end-system.

5. Remediation - When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that describes the compliance violations and provides remediations steps for the user to execute in order to achieve compliance. After taking the appropriate remediation steps, the end user clicks on a button on the web page to reattempt network access, forcing the re-assessment of the end-system. At this point, the Enterasys NAC solution transitions the end-system through the entire NAC cycle of detection, authentication, assessment, and authorization, re-assessing the security posture of the end-system to determine if the remediation techniques were successfully followed. If the end-system is now compliant with network security policy, the NAC Gateway authorizes the end-system with the appropriate access policy. If the end-system is not compliant, the end-system is restricted access to the network and the process starts again.

It is important to note that if the wireless edge of the network is non-intelligent and not capable of authenticating and authorizing wireless end-systems, it is possible to augment the network topology to implement out-of-band NAC with the NAC Gateway. This can be accomplished without replacing the physical edge of the network, by adding an intelligent edge switch that possesses specialized authentication and authorization features.

The Enterasys Matrix N-series switch is capable of authenticating and authorizing numerous end-systems connected on a single port through Multi-User Authentication (MUA), and may be positioned upstream from non-intelligent third-party wireless APs to act as the intelligent edge on the network. The Enterasys Matrix N-series switch is capable of authenticating and authorizing over 1000 end-systems uplinked to a single Matrix N-series port from an AP, a set of APs, or wireless switches. In this configuration, the Matrix N-series acts as the intelligent edge switch on the network, although not physically located on the access edge. By provisioning access to network resources on the Matrix N-series via MUA, end-system traffic destined to adjacent switches on the network can be securely contained at the Matrix N-series port.

Scenario 3: Non-intelligent Access Edge (Wired and Wireless)

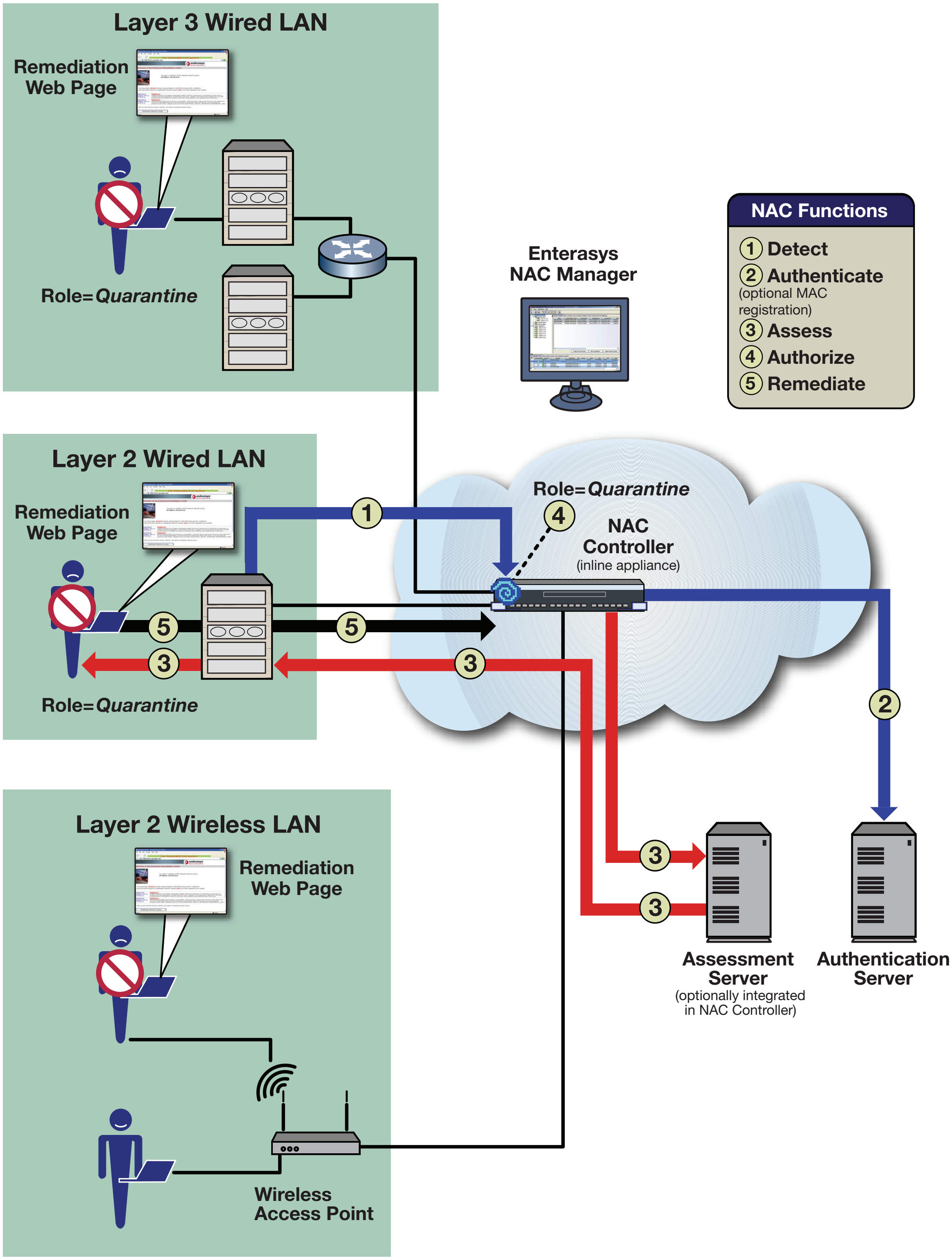
In the non-intelligent access edge use scenario, the edge switches and access points that compose the network access layer are **not** capable of authenticating and authorizing the connecting end-systems on the network.

In this scenario, inline NAC is implemented by positioning the NAC Controller at a strategic point in the network topology, as the authorization point for end-system traffic enforcement.

The NAC Controller may be positioned directly within the VLAN where end-systems are connected or across one or more routed boundaries. When the NAC Controller is positioned within the VLAN where end-systems are connected, each device is uniquely identified by its associated MAC address. When the NAC Controller is positioned across a routed boundary (for example, behind a WAN router located in an enterprise's central site), each end-system is identified by its associated IP address.

The following figure illustrates how the NAC Controller and the other Enterasys NAC components work together in the non-intelligent edge to provide network access control.

Figure 3-5 Non-intelligent Access Edge (Wired and Wireless)



Scenario 3 Implementation

In the non-intelligent access edge use scenario, the five NAC functions are implemented in the following manner:

1. Detection - The user's end-system connects to the network and transmits data traffic onto the network that traverses the NAC Controller. This traffic is sourced from a MAC address or IP address not previously seen by the controller.

2. Authentication - One of two configurations may be implemented on the NAC Controller for end user authentication. Authentication can be disabled altogether, trusting that the downstream infrastructure devices authenticated the end-system to the network (802.1X authentication to the wireless LAN, web-based authentication to the wired LAN). Alternatively, MAC registration can be implemented, where an end user username and password and/or sponsor username and password must be validated against a backend LDAP-compliant database before network access is permitted.

3. Assessment - After the identity of the end-system or end user is validated by authentication, the NAC Controller requests an assessment of the end-system according to predefined security policy parameters. The assessment can be agent-based or agent-less, and is executed locally by the NAC Controller's assessment functionality and/or remotely by a pool of assessment servers.

4. Authorization - Once authentication and assessment are complete, the NAC Controller allocates the appropriate network resources to the end-system based on authentication and/or assessment results. This is implemented locally on the NAC Controller by assigning a policy to traffic sourced from this end-system. If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC Controller can either deny the end-system access to the network or quarantine the end-system by specifying a particular policy on the NAC Controller.

5. Remediation - When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that describes the compliance violations and provides remediations steps for the user to execute in order to achieve compliance. After taking the appropriate remediation steps, the end user clicks on a button on the web page to reattempt network access, forcing the re-assessment of the end-system. At this point, the Enterasys NAC solution transitions the end-system through the entire NAC cycle of detection, authentication, assessment, and authorization, re-assessing the security posture of the end-system to determine if the remediation techniques were successfully followed. If the end-system is now compliant, the NAC Controller authorizes the end-system with the appropriate access policy. If the end-system is not compliant, the end-system is restricted access to the network by assigning a policy to the end-system on the NAC Controller, and the process starts again.

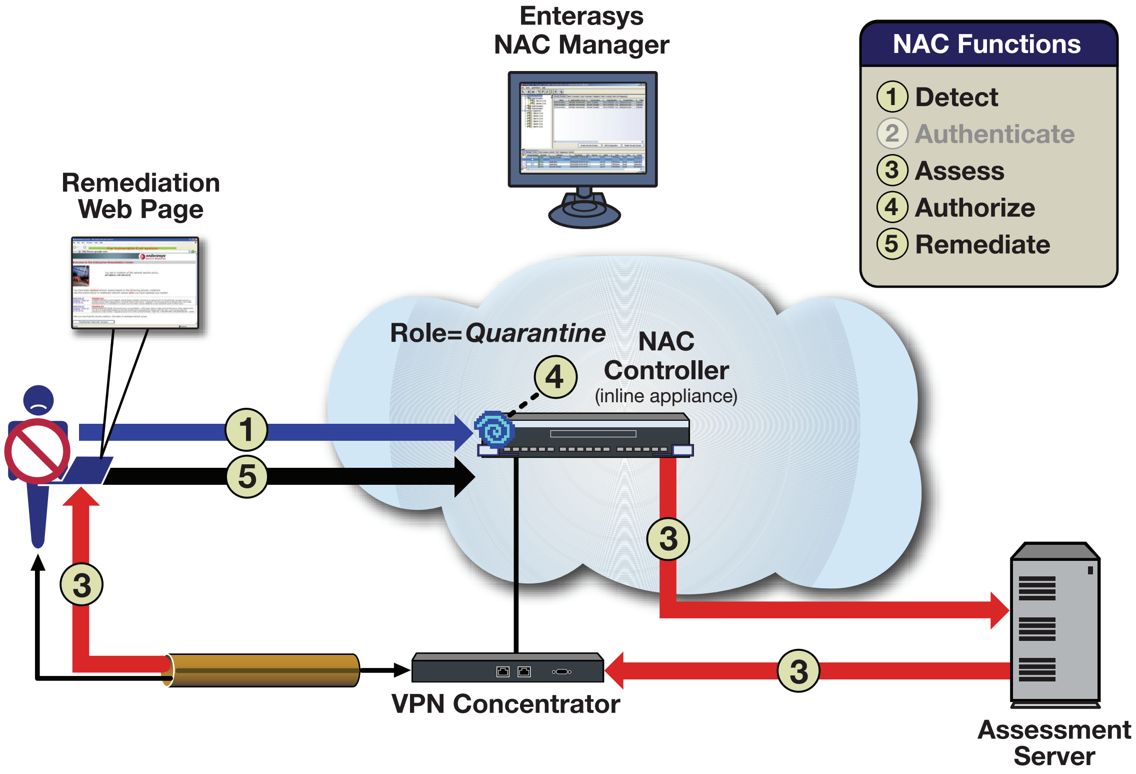
Scenario 4: VPN Remote Access

In the VPN remote access use scenario, VPN concentrators act as a termination point for remote access VPN tunnels into the enterprise network.

For this use scenario, the NAC Controller appliance is deployed to authorize connecting end-systems on the network and implement network access control.

The following figure illustrates how the NAC Controller and the other Enterasys NAC components work together in a VPN remote access deployment to provide a comprehensive NAC solution.

Figure 3-6 VPN Remote Access



Scenario 4 Implementation

In the VPN remote access use scenario, the five NAC functions are implemented in the following manner with the deployment of the NAC Controller for inline network access control.

1. Detection - The user's end-system successfully establishes a VPN tunnel with the VPN concentrator, and the VPN concentrator transmits unencrypted data traffic onto the network that traverses the NAC Controller. This traffic is sourced from an IP address not previously seen by the controller.

2. Authentication - Authentication is most likely disabled altogether on the NAC Controller, trusting that the downstream VPN concentrator authenticated the connecting user.

3. Assessment - The NAC Controller requests an assessment of the end-system according to predefined security policy parameters. The assessment can be agent-based or agent-less, and is executed locally by the NAC Controller's assessment functionality and/or remotely by a pool of assessment servers.

4. Authorization - Once authentication and assessment are complete, the NAC Controller allocates the appropriate network resources to the end-system based on authentication and/or assessment results. This is implemented locally on the NAC Controller by assigning a policy to traffic sourced from the end-system. If authentication fails and/or the assessment results indicate a noncompliant end-system, the NAC Controller can either deny the end-system access to the network, or quarantine the end-system by assigning a particular policy on the controller.

5. Remediation - When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that describes the compliance violations and provides remediations steps for the user to execute in order to achieve compliance. After taking the appropriate remediation steps, the end user clicks on a button on the web page to reattempt network access, forcing the re-assessment of the end-system. At this point, the Enterasys NAC solution transitions the end-system through the entire NAC cycle, re-assessing the security posture of the end-system to determine if the remediation techniques were successfully followed. If the end-system is now compliant with network security policy, the NAC Controller authorizes the end-system with the appropriate access policy. If the end-system is not compliant, the end-system is restricted access to the network by assigning a policy to the end-system on the NAC Controller, and the process starts again.

Summary

The decision whether to deploy inline or out-of-band network access control depends on the infrastructure devices deployed in your network. For some network topologies, inline NAC utilizing the NAC Controller appliance may be required while for other network configurations, out-of-band NAC utilizing the NAC Gateway appliance may be used.

The following table summarizes four NAC use scenarios and their NAC appliance requirements. The Enterasys NAC solution is capable of implementing network access control for all four use scenarios as well as environments with mixed use scenarios that may require the concurrent deployment of inline and out-of-band NAC.

Table 3-1 Use Scenario Summaries

Use Scenario	Summary and Appliance Requirements
Scenario 1: Intelligent wired access edge	**Summary:** Intelligent edge switches in the network access layer provide authentication and authorization for connecting end-systems. **Appliance Requirement: NAC Gateway** The NAC Gateway appliance provides out-of-band network access control by leveraging the intelligent edge switches as the authorization point for connecting end-systems.
Scenario 2: Intelligent wireless access edge	**Summary:** Thick Access Points (APs), or wireless switches with thin APs, provide authentication and authorization for connecting end-systems. **Appliance Requirement: NAC Gateway** The NAC Gateway appliance provides out-of-band network access control by leveraging the intelligent wireless infrastructure devices as the authorization point for connecting end-systems.
Scenario 3: Non-intelligent access edge (wired and wireless)	**Summary:** Non-intelligent edge switches in the network access layer are **not** capable of providing authentication and authorization for connecting end-systems. **Appliance Requirement: NAC Controller** Inline network access control is implemented by positioning the NAC Controller appliance at a strategic point in the network topology as the authorization point for end-system traffic.

Table 3-1 Use Scenario Summaries (continued)

Use Scenario	Summary and Appliance Requirements
Scenario 4: VPN remote access	**Summary:** VPN concentrators act as a termination point for remote access VPN tunnels into the enterprise network. **Appliance Requirement: NAC Controller** Inline network access control is implemented by deploying the NAC Controller appliance to locally authorize connecting end-systems.

4

Design Planning

This chapter describes the steps you should take as you begin planning your NAC deployment. The first step is to identify the deployment model that best meets your business objectives. Then, the current network infrastructure must be evaluated in order to determine NAC component requirements. Based on this evaluation, you will be able to decide whether to deploy inline or out-of-band network access control.

Identify the NAC Deployment Model

When planning your NAC deployment, the first step is to identify the NAC deployment model, or a phased implementation of multiple deployment models, that meets your NAC business objectives. The four deployment models are summarized below. For more in depth information on each model, see Chapter 2, NAC Deployment Models.

- Model #1: End-System Detection and Tracking

  Enterasys NAC detects devices as they connect to the network, identifying the location, MAC address, IP address, and username of the person using the end-system. This information is maintained over time for each device on the network, yielding complete historical information about a device as it interacts with the network.

- Model #2: End-System Authorization

  Enterasys NAC detects, authenticates, and authorizes connecting end-systems, to control access to network resources based on location as well as user and end-system identity.

- Model #3: End-System Authorization with Assessment

  Enterasys NAC is deployed with end-system assessment and authorization (but without remediation), to control access to network resources based on the security posture of a connecting end-system. Compliant end-systems are permitted onto the network, while end-systems that fail assessment can be dynamically quarantined with restrictive network access.

- Model #4: End-System Authorization with Assessment and Remediation

  In addition to end-system assessment and authorization, Enterasys NAC is deployed with remediation to dynamically inform quarantined end-systems of security compliance violations. Using web-based notification, assisted remediation allows end users that have access to a web browser to safely remediate their quarantined end-system without impacting IT operations.

Once a deployment model is selected, the current network infrastructure must be examined to identify the technical dependencies and requirements imposed by the NAC solution.

Survey the Network

The steps in this section will help you identify and evaluate the current network infrastructure so that you can make design decisions regarding NAC component requirements.

1. Identify the Intelligent Edge of the Network

The first step in surveying your network is to determine whether or not your network has an "intelligent edge." This information will help you decide whether the NAC Gateway or NAC Controller appliance best suits your network infrastructure.

The term "intelligent" refers to a network topology where the access edge is composed of Enterasys policy-enabled switches capable of supporting authentication and policy enforcement, or third-party switches capable of supporting authentication and dynamic VLAN assignment as defined in RFC 3580.

Non-intelligent infrastructure devices, such as repeaters and hubs, are not capable of supporting authentication and/or authorization of end-systems, and simply provide connectivity to the infrastructure.

An intelligent edge is required when the NAC Gateway is utilized for implementing out-of-band NAC. The NAC Gateway appliance leverages the intelligent edge of the network to implement the authentication and authorization of connecting end-systems. The NAC Gateway effects the assignment of policies or VLANs on Enterasys switches or RFC 3580-capable switches located at edge of the network, to authorize a level of network access to connecting end-systems. These assignments are based on various parameters, such as the location of the end-system and security posture assessment results. The intelligent edge of the network also implements an authentication method (802.1X, web-based, or MAC authentication) for validating the device and/or user identity of connecting end-systems.

However, in networks with non-intelligent devices at the access edge, it is not necessary to replace these non-intelligent devices to be able to implement out-of-band NAC with the NAC Gateway. Instead, the Enterasys Matrix N-series switch can be positioned upstream from non-intelligent devices (such as in the distribution layer) to implement the authentication and authorization functions for downstream connected devices. Matrix N-Series devices support Multi-User Authentication (MUA) which enables the switch to individually authenticate and uniquely authorize multiple end-systems connected to the same physical port. MUA on the Matrix N-series Platinum supports the concurrent authentication and authorization of over 1000 end-systems on a single port with the allocation of disparate network resources to each end-system. In this case, the Matrix N-series switch is the intelligent edge of the network although it is not physically located in the access layer. By utilizing the Matrix N-series in this type of configuration, most of the benefits of out-of-band NAC can be obtained without upgrading the edge of the network.

The network shown in Figure 4-1 below, illustrates the following three examples of how the intelligent edge can be implemented in a network.

- **Policy-enabled Enterasys devices at the physical edge of the network.**

  The SecureStack B2/B3, SecureStack C2/C3, and Matrix N-series switches are the intelligent edge of the network as well as the physical edge of the network. These policy-enabled devices provide authentication and authorization via policy enforcement to the connecting end-systems.

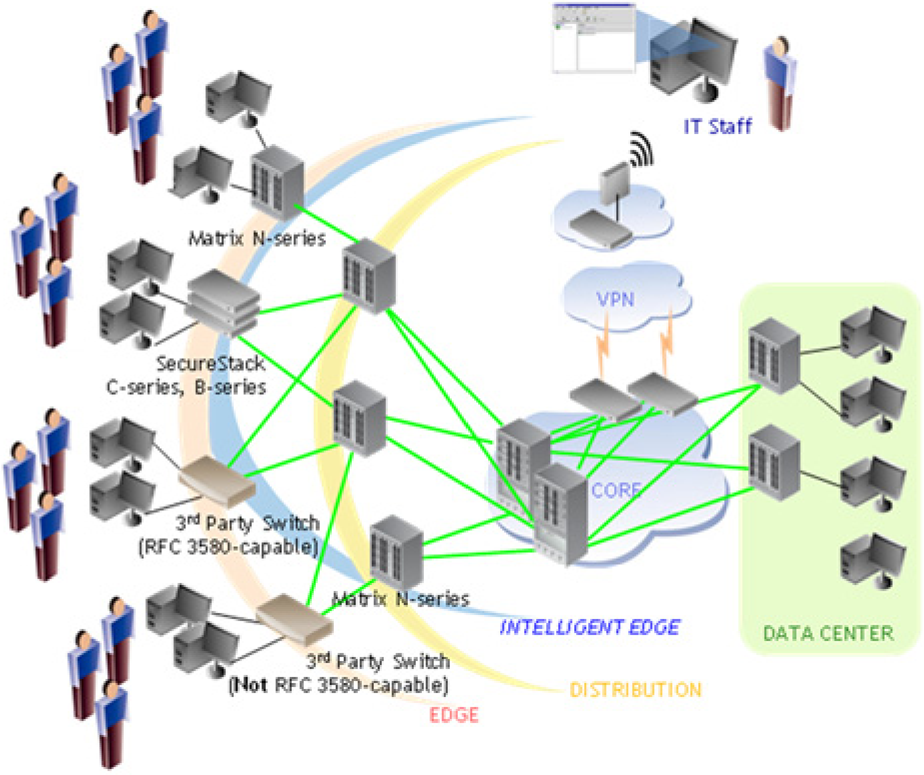
- **Third-party switches that support RFC 3580 with dynamic VLAN assignment at the physical edge of the network.**

  RFC 3580-compliant switches (Enterasys and third-party), are also part of the intelligent edge of the network, because they are able to authenticate and authorize connecting end-systems with a particular level of network access, using dynamic VLAN assignment.

- **Policy-enabled Enterasys devices at the distribution layer of the network, upstream from non-intelligent third-party devices.**

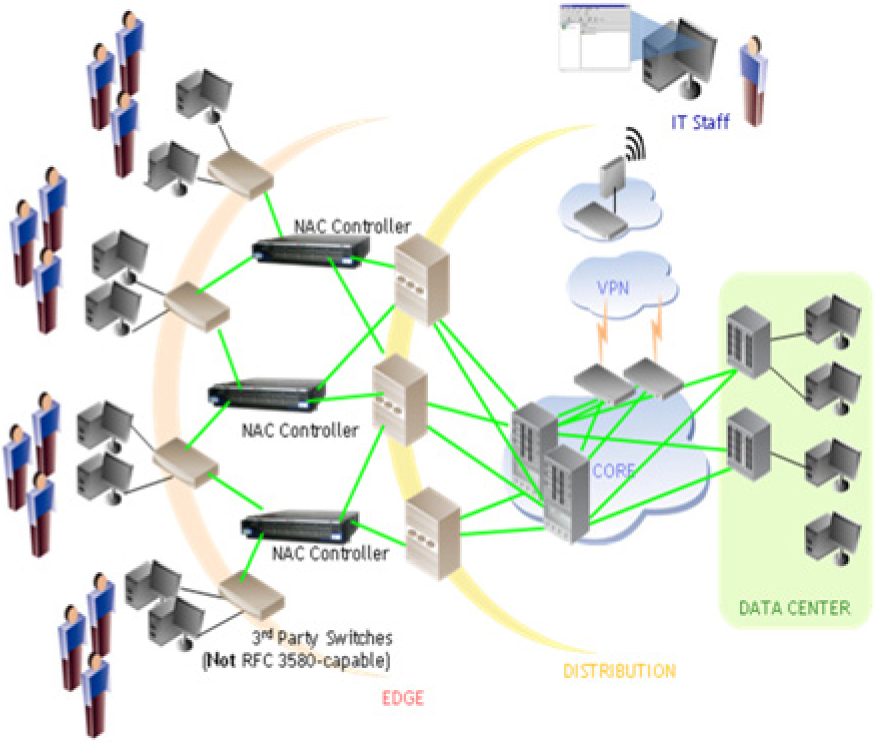
  The intelligent edge of the network may or may not be the physical edge of the network where end-systems actually connect. The Matrix N-series switch in the distribution layer of the network, upstream from the non-intelligent third-party device, is also considered part of the intelligent edge of the network. This is because the Matrix N-series switch can individually authenticate and uniquely allocate network resources for the end-systems connected downstream to the non-intelligent third-party access layer device.

Figure 4-1 Network with Intelligent Edge



For the inline implementation of the Enterasys NAC solution, the NAC Controller authenticates and authorizes end-systems locally on the appliance, and does not rely on the capabilities of downstream infrastructure devices. Because of this, the NAC Controller can be utilized in networks where non-intelligent and/or intelligent infrastructure devices exist at the edge of the network. If the network does not have an intelligent edge, then the NAC Controller must be deployed in order to provide the authentication and authorization capabilities required for implementing network access control, as shown in Figure 4-2.

Figure 4-2 Network with Non-Intelligent Edge



2. Evaluate Policy/VLAN and Authentication Configuration

Note: This step is not necessary if in step 1 you determined that the network does not have an intelligent edge and the inline NAC Controller appliance will be deployed to provide the authentication and policy enforcement capabilities.

For a network with an intelligent edge, the second step in surveying your network is to evaluate the network authentication method currently being used, and how the deployment of Enterasys NAC will affect it. A network with an intelligent edge can be classified into one of two cases: either authentication is deployed on the network or it is not.

Case #1: No authentication method is deployed on the network.

If authentication is not configured on the network, out-of-band NAC can be deployed with minimal configuration by implementing MAC authentication on the intelligent edge of the network (if the edge switches support MAC authentication). The NAC Gateway can be configured to locally authorize all MAC authentication requests for connecting end-systems, thereby not requiring a list of known MAC addresses. In fact, Enterasys NAC can be configured in a “learning mode” to dynamically learn the MAC addresses of all devices connecting to the network, permitting network access to all of these end-systems for a period of time.

After the MAC addresses are learned, NAC can be reconfigured to permit access only to these end-systems, requiring all other devices connecting to the network to go through a registration process.

With MAC authentication deployed on the network, a backend RADIUS server with associated directory services is not required, simplifying the implementation. Furthermore, because MAC authentication only requires the end-system to generate an Ethernet packet onto the network, both human-centric and machine-centric end-systems have the capability to authenticate to the network, regardless of whether the end-system is a PC or a printer.

Case #2: Authentication methods are deployed on the network.

If authentication is currently deployed on the network with 802.1X, web-based, and/or MAC authentication, then a RADIUS server with associated backend directory services must be deployed for user/device 802.1X and web-based credential validation. Moreover, if RADIUS authentication for switch management logins is implemented, a RADIUS server must be deployed on the network. In this scenario, out-of-band NAC is configured to seamlessly proxy RADIUS authentication requests received from the switches at the intelligent edge of the network to the backend RADIUS server, without requiring complex configuration changes to the RADIUS server and associated directory services. In addition, NAC can also be configured to locally authorize MAC authentication requests.

Overview of Supported Authentication Methods

Following is an overview of authentication methods supported by Enterasys and some third-party switches, and proxied by out-of-band NAC.

802.1X Authentication

The IEEE 802.1X standard for port-based network access control, provides network administrators with the ability to authenticate and authorize an end user at the port level.

The 802.1X authentication method is usually implemented on PCs in secure environments and requires that the end-system implement an 802.1X supplicant, which is special software that communicates in this protocol.

Because 802.1X requires the input of user credentials, 802.1X is normally used on user-centric end-systems that have a concept of an associated user, such as a PC. Therefore, this authentication method may be inappropriate for machine-centric devices, such as printers and IP cameras. However, newer software releases for IP phones may include an 802.1X supplicant.

Since Enterasys NAC only acts as a pass-through to an upstream RADIUS Server, it is mandatory that a full authentication deployment is configured on the network if 802.1X is used.

Web-Based Authentication

Web-based authentication, or Port Web Authentication (PWA), is an authentication process that uses a web browser, user-login process to gain access to ports. It employs either CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol).

Since web-based authentication only requires that a web browser is on the end-system, it is deployed in heterogeneous environments where certain end-systems may not have an 802.1X supplicant installed.

Similar to 802.1X, web-based authentication requires the input of credentials and is normally used on user-centric end-systems that have a concept of an associated user, such as a PC. Therefore, this authentication method is inappropriate for machine-centric devices such as printers and IP cameras.

Note that web-based authentication is a user-initiated authentication method where the user must manually begin the network login process by opening a web browser and entering credentials. This user-initiated method prevents seamless network connectivity because the end user must initiate the reauthentication after assessment is complete.

Since Enterasys NAC only acts as a pass-through to an upstream RADIUS Server, it is mandatory that a full authentication deployment is configured on the network if web-based authentication is used.

MAC Authentication

MAC authentication authenticates the source MAC address of an end-system and grants the appropriate level of access by validating the MAC address on the RADIUS authentication server.

This authentication method only requires that the end-system generate a packet; it requires no special software on the end-system.

Unlike 802.1X and web-based authentication, MAC authentication can be used to authenticate machine-centric end-systems that have no concept of an associated user, such as a printer or IP camera.

With this authentication method, Enterasys NAC can act as a pass-through to an upstream RADIUS Server or can locally authorize MAC authentication attempts. Therefore, if a full authentication deployment has not been configured on the network, MAC authentication should be used.

End-System Capabilities

When authentication is configured on the network, it is important to consider end-system capabilities and their ability to interact with the authentication process. Machine-centric end-systems that do not possess an 802.1X supplicant, such as IP cameras and printers, may only be capable of MAC authenticating to the network. Some human-centric end-systems such as PCs, may be capable of 802.1X and web-based authentication while other PCs not installed with an 802.1X supplicant, are only capable of web-based authentication. If end-systems are implementing 802.1X and web-based authentication, Enterasys NAC should leverage these authentication methods for end-system detection. For end-systems not implementing 802.1X or web-based authentication, MAC-based authentication can be enabled on these switch ports.

Support of Multiple Authentication Methods

In order to support an enterprise network consisting of a diverse environment of machine-centric and human-centric devices, it is important that the intelligent edge of the network supports the concurrent enabling of multiple authentication methods, all at the same time on the same switch port. Some intelligent switches may not support the enabling of multiple authentication methods concurrently on a single port. For example, MAC and 802.1X authentication may be concurrently enabled on a port to account for the fact that a trusted user, guest user, or IP phone may connect to this port. The ability to support multiple authentication methods concurrently on a port is even more important for environments where mobility of devices around the network is essential for ensuring business continuity.

Support for Multiple End-System Connection

It is important to know whether multiple end-system connection is supported by the intelligent edge of the network. If the intelligent edge devices only support the authentication of one end-system at a time, then it is suggested that MAC locking (also known as Port Security) be enabled on the edge switches to restrict the number of connecting devices. If multiple end-system connection is supported, then the intelligent edge switch must support the authentication and authorization of multiple devices (possibly using multiple authentication methods) concurrently on the network. If this is not supported, then a security hole exists where a noncompliant end-system can “piggyback” on the open network connection of a compliant end-system.

For example, NAC is often deployed on an IP telephony converged network where IP phone handsets are cascaded with PCs connected to a single intelligent edge infrastructure port. If the intelligent edge infrastructure devices do not support the authentication and authorization of both the PC and IP phone connected to the same port, then a noncompliant PC may be allowed network access when the security posture of an IP phone that connected to the network first, is deemed compliant.

Furthermore, if the authentication and authorization of multiple devices connecting to a single port is not supported, certain devices may lose connectivity when NAC is deployed. For example, an IP phone's network connection may be lost when a PC is quarantined on the network.

Authentication Support on Enterasys Devices

Following is information on the authentication support provided by Enterasys devices:

- The Matrix N-series Multi-User Authentication (MUA) feature allows the enabling of any combination of authentication methods (802.1X, web-based, and/or MAC) both globally and per port. While the Matrix N-series Gold supports the authentication and authorization of two users/devices per port, the Matrix N-series Platinum supports the authentication and authorization of over 2000 users and devices per port, providing the highest degree of authentication method configuration flexibility.
- The SecureStack C2/C3 and B2/B3 User + IP Phone authentication allows the configuration of multiple authentication methods globally and per port (802.1X, web-based, and/or MAC) with the limitation of a PC and an IP phone authenticating on a single port.
- The Matrix E1's Hybrid authentication allows the enabling of both 802.1X and MAC authentication on the same port, and supports the authentication of a single end-system using only one of these authentication methods at a time.
- If web-based authentication is globally enabled on the Matrix E1 and the Matrix E-series Generation 2/3 platforms, each port on the switch can only be configured to implement web-based authentication.

Authentication Considerations

If authentication is currently deployed on the network, here are considerations that should be reviewed as you plan your NAC deployment:

- Enterasys NAC will seamlessly integrate with deployments where the authenticating and authorization of trusted users is already implemented. Enterasys NAC can be configured to forward the RADIUS Filter-ID and/or VLAN Tunnel attribute returned from the RADIUS server to the access layer switch during the authentication process.
- If guest access is implemented on the network by assigning a default policy or VLAN on certain ports (assuming guest users will fail authentication on the network), the infrastructure will need to be reconfigured to implement NAC for guest users. Enterasys NAC will not assess or authorize end-systems that only fail authentication against a backend RADIUS server. To enable Enterasys NAC to interact with guest users on the network, MAC authentication must be enabled on ports where guest users connect to the network, and Enterasys NAC must be configured to locally authorize MAC authentication requests and assign the appropriate guest authorization level. Then, guest users will be successfully MAC

authenticated to the network and interact with Enterasys NAC for authentication, assessment, authorization, and remediation. Note however, that this configuration may not be possible if trusted users are also being MAC authenticated to the network in the same Security Domain. In this case, MAC or user overrides would need to be configured for the trusted users, and the default NAC configuration of the Security Domain would specify the NAC implementation for guest users.

- If guest access is implemented with web-based authentication using the guest networking feature on Enterasys policy-capable switches (supplying default credentials in the web login page for guest users), the guest networking feature must be configured to send the default credentials to a backend RADIUS server and not locally authenticate them. This is because in the out-of-band NAC configuration, the NAC Gateway must receive the authentication attempt via RADIUS in order to detect the connecting end-systems. A RADIUS server with the guest networking credentials must be deployed on the network so the NAC Gateway can proxy the RADIUS requests to the upstream RADIUS server. If a RADIUS Filter-ID or VLAN Tunnel attribute is not configured for the guest networking credentials on the upstream RADIUS server, Enterasys NAC can be configured to include a Filter-ID or VLAN Tunnel attribute in the RADIUS Access-Accept packet returned to the switch by implementing a user override for the guest networking username.

3. Identify the Strategic Point for End-System Authorization

In this step, you will identify the strategic point in the network where end-system authorization should be implemented.

The most secure place for implementing authorization is directly at the point of connection at the edge of the network, as supported by Enterasys policy-capable switches. In this configuration, the implementation of out-of-band NAC using the NAC Gateway appliance leverages policy on Enterasys switches to securely authorize connecting end-systems.

RFC 3580-capable switches can be used for authentication and authorization by assigning end-systems to particular VLANs based on the authentication and assessment results. However, this is not as secure as using Enterasys policy-capable switches, for the two following reasons:

- VLANs authorize end-systems by placing them into the same container, with the traffic enforcement point implemented at the ingress/egress point to the VLAN on the VLAN's routed interface. Because authorization is not implemented between end-systems within the same VLAN, an end-system in a VLAN is open to launch attacks or be attacked by other devices within the same VLAN. For example, if end-system A with virus X and end-system B with virus Y are quarantined into the same VLAN, then end-system A and B may become infected with virus X and Y. Enterasys policy uniquely authorizes connecting end-systems independent of their VLAN assignment by permitting, denying, and prioritizing traffic on ingress to the network at the port level.
- Because RFC 3580-capable switches implement the traffic enforcement point for a VLAN at the VLAN’s routed interface, malicious traffic is allowed onto the network and may consume bandwidth, memory, and CPU cycles on infrastructure devices before being discarded possibly several hops deep within the network. This is especially detrimental to the operation of the network if a single inter-switch link connecting the access layer to distribution layer is used to transmit traffic from both the quarantine VLAN and the production VLAN (such as an 802.1Q VLAN trunked link). Traffic from quarantined end-systems (for example, worms scanning for vulnerable hosts) can consume the entire bandwidth available on the inter-switch link and affect network connectivity for end-systems on the production VLAN. In contrast, since the traffic enforcement point for Enterasys policy is at the port of connection, malicious traffic never ingresses the network to cause any disruption to network connectivity.

If the network infrastructure does not contain intelligent devices at the edge or distribution layer, then inline NAC using the NAC Controller as the authorization point for connecting end-systems must be implemented. This is not as secure as out-of-band NAC because the authorization point for end-systems is located deeper into the network at the NAC Controller. With inline NAC, a quarantined end-system, while restricted from network access to resources upstream from the NAC Controller, is still able to interact openly with resources and assets on the network downstream from the NAC Controller. However, an advantage of the NAC Controller is that it provides network access control without requiring the upgrade of the access layer or distribution layer of the network.

Furthermore, it is important to note that the NAC Controller and NAC Gateway can be deployed concurrently in the network for the simultaneous implementation of inline and out-of-band NAC, all centrally managed from the NetSight NAC Manager. The NAC Gateway can be utilized for areas of the network where intelligent switches reside, while the NAC Controller can be positioned inline for segments of the network where non-intelligent devices exist.

If the deployment of out-of-band NAC is desired for a network with non-intelligent access layer devices, the following options should be considered:

- Distribution layer infrastructure devices can be strategically upgraded to Enterasys Matrix N-Series devices that are capable of individually authenticating and uniquely authorizing multiple devices connected to a single port. Most of the security benefits of out-of-band NAC using Enterasys policy can be obtained by implementing authorization at the distribution layer instead of at the port of connection in the access layer.
- Access layer infrastructure devices can be upgraded to Enterasys policy-capable switches or RFC 3580-capable switches to obtain the security benefits of out-of-band NAC.

4. Identify Network Connection Methods

The previous steps have been concerned with implementing NAC for the internal LAN. In this step, various types of network connection methods are discussed, along with their impact on NAC deployment.

Wired LAN

Out-of-band or inline NAC can be implemented, depending on the capabilities of the access edge infrastructure devices.

Wireless LAN

Wireless LAN deployments may be categorized into either thick wireless deployments where access points (APs) operate independently on the network, or thin wireless deployments where APs communicate back to centrally deployed wireless switches that facilitate communication between APs.

Thick Wireless Deployments

Thick wireless deployments may consist of full-featured APs that support authentication and authorization. Full-featured thick APs fall into the intelligent edge category and have the same NAC implications as an intelligent wired edge. In this case, intelligent APs in a thick wireless deployment can be configured with out-of-band NAC using the NAC Gateway, with authentication and authorization implemented on the thick APs.

Other thick AP deployments may consist of APs that do not support authentication and/or authorization and merely act as a media converter between the wireless and wired networks. In this case, the thick AP deployment falls into the category of non-intelligent edge devices with the same NAC implementations as a non-intelligent wired edge. These non-intelligent APs must be configured with inline NAC, positioning the NAC Controller at a strategic point in the network upstream from the non-intelligent APs where it will implement the authentication and authorization of connecting end-systems.

Thin Wireless Deployments

For thin wireless deployments, the wireless switch usually supports the authentication and authorization of the wireless end-systems connected to the APs on the network. Therefore, thin wireless deployments can be configured with out-of-band NAC using the NAC Gateway, with the authentication and authorization implemented on the wireless switch. If the wireless switch does not support dynamic VLAN assignment via RFC 3580, inline NAC may be used by positioning the NAC Controller behind the wireless switch to implement the authentication and authorization of wireless end-systems.

Remote Access WAN

In many enterprise networks, larger remote sites are connected to the main network site over a WAN connection, affording remote users access to corporate resources. If the remote sites are composed of intelligent edge devices supporting the authentication and authorization of the remotely connected end-systems, then the NAC Gateway can be utilized in the deployment of out-of-band NAC. The NAC Gateway may be positioned either locally at the remote site (which may not be practical) or at the main site of the enterprise network. Either way, the NAC Gateway leverages the authentication and authorization capabilities of the switches in the remote site to implement network access control for remote users.

If the NAC Gateway is implemented at the main site, then it is important to consider what impact a WAN link disconnection would have on the NAC process and remote end-system connectivity. It is recommended that switches in remote sites be configured with a default VLAN or policy that will be applied to the end-system in the case that connectivity to the main site goes down.

If the remote sites are composed of non-intelligent switches, then the NAC Controller can be strategically positioned inline with traffic sourced from remote end-systems to implement the authentication and authorization of these devices. The NAC Controller is most often positioned at the central site's WAN connection to the remote sites. In this configuration, the NAC Controller is able to implement NAC for multiple remote sites, which is important when you consider that some remote sites may have only a few end-systems concurrently connected.

Site-to-Site VPN

In multi-site enterprise environments, it is common to have a VPN concentrator located at the main site connecting to remote sites via a VPN tunnel. Similar to the remote access WAN scenario, the implementation of out-of-band or inline NAC depends on the capabilities of the edge switches located at the remote site. If the remote sites are composed of intelligent edge switches, then the NAC Gateway can be positioned at the main site to implement out-of-band NAC. If the remote sites are composed of non-intelligent edge switches, then the NAC Controller can be positioned behind the VPN concentrator that provides site-to-site VPN connectivity. It is important to note that the NAC Controller must see the actual IP address of the end-system when an end-system's traffic traverses it. Therefore, a downstream device from the NAC Controller cannot implement many-to-one NAT or reverse proxy VPN, so that the IP address of the end-system is preserved at the point that the traffic traverses the NAC Controller.

Remote Access VPN

In many enterprise environments, a VPN concentrator located at the main site connects to the Internet to provide VPN access to remote users. In this scenario, there is no concept of intelligent and non-intelligent edge switches because the entry point to the main site is the VPN concentrator. In this scenario, the NAC Controller must be used to implement NAC for remote access VPN end-systems, and it should be positioned behind the VPN concentrator that provides remote access VPN. Again, reverse proxy VPN or many-to-one NAT implemented on a downstream device from the NAC Controller is not supported in the Enterasys NAC solution.

Identify Inline or Out-of-band NAC Deployment

Based on the NAC deployment model you selected, and the results of your network infrastructure evaluation, you must identify whether out-of-band NAC or inline NAC will be deployed in the different areas of your network. With the decision to implement out-of-band NAC with the NAC Gateway, and/or inline NAC with the NAC Controller, the next design step is to determine your specific enterprise requirements for the selected NAC solution, and identify the number of NAC appliances, and their location and configuration on the network.

Summary

The first step when planning your NAC deployment, is to identify the NAC deployment model, or a phased implementation of multiple deployment models, that meets your NAC business objectives. Once you have selected a deployment model, you can use the four following steps to evaluate your current network infrastructure and determine your NAC component requirements.

1. Identify the “intelligent edge” in your network, if it exists. This information will be used to help you select which NAC appliance, the NAC Gateway or NAC Controller, best suits your network infrastructure.

   An intelligent edge is required when the NAC Gateway is utilized for implementing out-of-band NAC. The NAC Gateway appliance leverages the intelligent edge of the network to implement the authentication and authorization of connecting end-systems.

   In networks with non-intelligent devices at the access edge, it is not necessary to replace these non-intelligent devices to be able to implement out-of-band NAC with the NAC Gateway. Instead, the Enterasys Matrix N-series switch can be positioned upstream from non-intelligent devices (such as in the distribution layer) to implement the authentication and authorization functions for downstream connected devices.

   If the network does not have an intelligent edge, then the NAC Controller must be deployed in order to provide the authentication and authorization capabilities required for implementing network access control.

2. Evaluate the network authentication method currently being used, and how the deployment of Enterasys NAC will affect it. (This step is not required if you have determined that the network does not have an intelligent edge and the inline NAC Controller will be deployed.)

   If authentication is not configured on the network, out-of-band NAC can be deployed with minimal configuration by implementing MAC authentication on the intelligent edge of the network (if the edge switches support MAC authentication).

   If authentication is currently deployed on the network with 802.1X, web-based, and/or MAC authentication, out-of-band NAC is configured to proxy RADIUS authentication requests received from the switches at the intelligent edge of the network to the backend RADIUS server. In addition, NAC can also be configured to locally authorize MAC authentication requests.

3. Identify the strategic point in the network where end-system authorization should be implemented.

   The most secure place for implementing authorization is directly at the point of connection at the edge of the network, as supported by Enterasys policy-capable switches. In this configuration, the implementation of out-of-band NAC using the NAC Gateway appliance leverages policy on Enterasys switches to securely authorize connecting end-systems.

   If the network infrastructure does not contain intelligent devices at the edge or distribution layer, then inline NAC using the NAC Controller as the authorization point for connecting end-systems must be implemented.

4. Identify the network connection types being used. The previous steps have been concerned with implementing NAC for the internal LAN. In this step, the following connection types are discussed along with their impact on the Enterasys NAC solution.

   – Wired LAN

   – Wireless LAN

   – Remote Access WAN

   – Site-to-Site VPN

   – Remote Access VPN

Based on the NAC deployment model you select, and the results of your network infrastructure evaluation, you will be able to identify whether out-of-band NAC or inline NAC will be deployed in the different areas of your network.

5

Design Procedures

This chapter describes the design procedures for Enterasys NAC deployment on an enterprise network. The first section discusses procedures for both out-of-band and inline NAC deployments. The second section discusses procedures for deployments implementing assessment. Subsequent sections present design steps relating specifically to out-of band deployments using the NAC Gateway and inline deployments using the NAC Controller.

Procedures for Out-of-Band and Inline NAC

This section presents design procedures that are applicable to both out-of-band and inline NAC deployments.

1. Identify Required NetSight Applications

As discussed in "NetSight Management" on page 1-9, the Enterasys NAC solution requires the installation of two applications from the NetSight management software suite. NetSight NAC Manager is required to centrally manage the NAC Controller and NAC Gateway appliances on the network. Because NAC Manager is a plugin application to NetSight Console, it is necessary to have NetSight Console installed on a server with NAC Manager. NetSight Console is used to monitor the health and status of devices on the network, including the access layer switches and the NAC appliances.

In addition, NetSight Policy Manager is required for inline NAC deployments. Policy Manager is used to centrally define and distribute policies to all NAC Controllers on the network.

For out-of-band NAC deployments that include Enterasys policy-enabled switches in the intelligent edge, policies are specified in NAC Manager that authorize connecting end-systems with a particular level of network access. Policies are centrally defined and distributed to those Enterasys switches using Policy Manager. With Policy Manager, policy roles are easily defined and enforced to all Enterasys switches in the entire intelligent edge of the network, from one central location.

Policy Manager is not required for out-of-band NAC that utilizes RFC 3580-compliant switches (Enterasys and third-party switches). In this case, a VLAN is specified in NAC Manager to authorize connecting end-systems with a particular level of network access, using dynamic VLAN assignment.

Refer to the Enterasys Networks web site http://www.enterasys.com/products/management/downloads/NetSight.html for NetSight software licensing and download information.

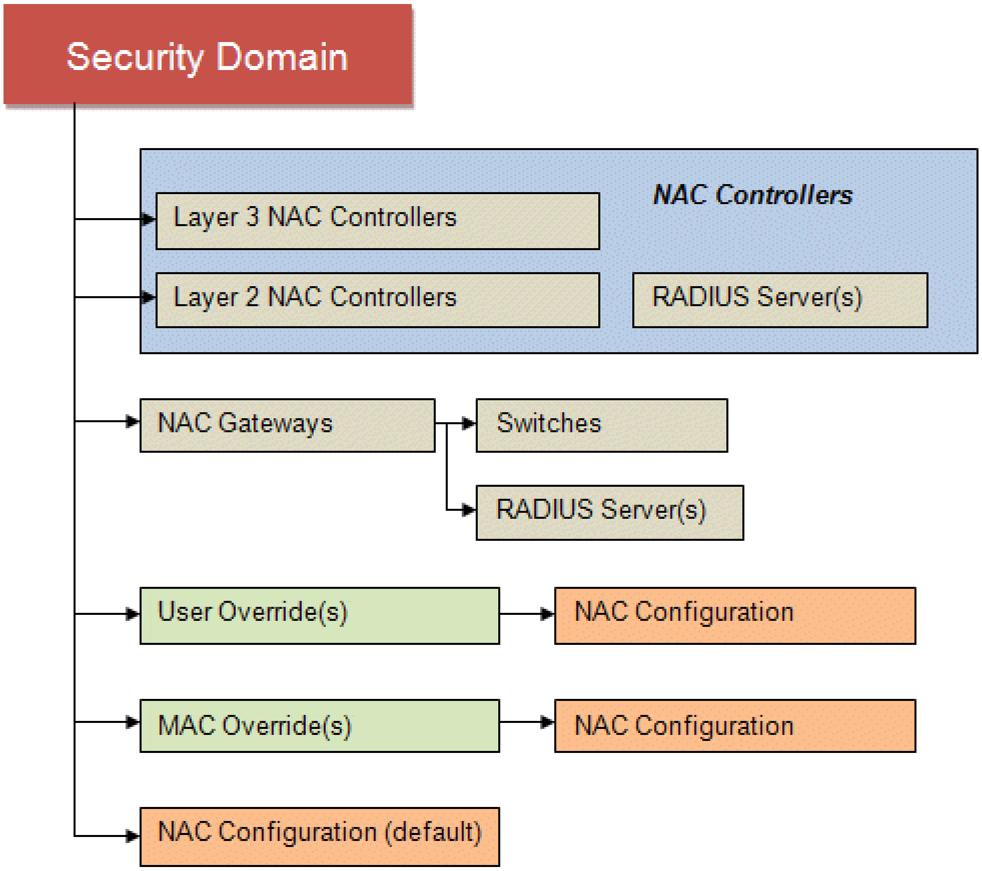
2. Define Network Security Domains

A different Security Domain should be defined for each area of the network that has its own unique requirements for end-system authentication, assessment, and authorization.

A Security Domain defines a set of NAC Gateways and NAC Controllers that have common authentication, assessment, and authorization requirements for end-systems connecting to the network. For NAC Gateways, the domain also includes the associated switches that are uniquely assigned to the gateways.

A Security Domain can be composed of both NAC Controller and NAC Gateway appliances. Each NAC Gateway can only be assigned to one Security Domain and therefore all ports on a particular switch (for example, a stack of SecureStack C2 switches or a Matrix N7 chassis) can only be associated to one Security Domain. Likewise, a NAC Controller can only be assigned to one Security Domain.

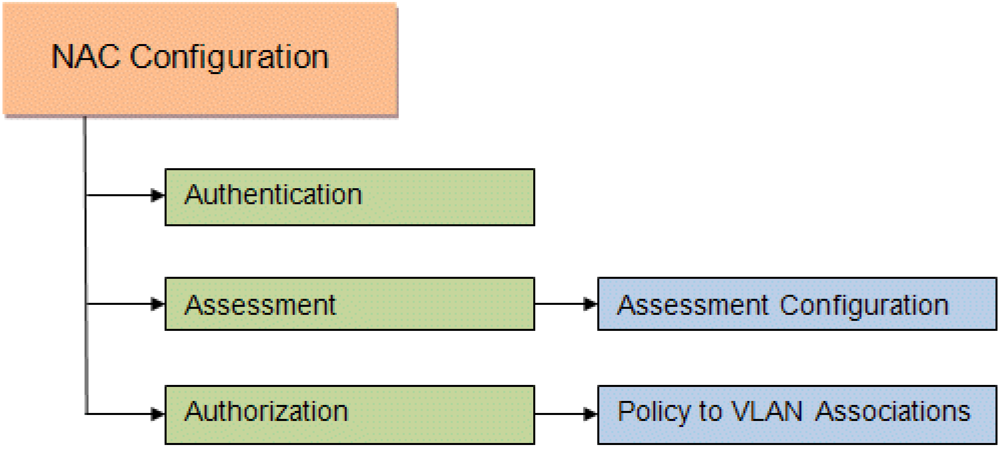
Figure 5-1 Security Domain



NAC Configurations

Each Security Domain has a default "NAC configuration" that defines the authentication, assessment, and authorization parameters for all end-systems connecting in that domain. A Security Domain can also include MAC or user override rules that are used to override the NAC configuration parameters with a special NAC configuration to be used for specific end-systems or end users.

Figure 5-2 NAC Configuration



Authentication

The Authentication settings define how RADIUS requests are handled for authenticating end-systems (this does not apply to Layer 3 NAC Controllers.) This includes identifying whether MAC authentication requests are proxied upstream or locally authorized, and whether Filter-ID and Tunnel RADIUS attributes are added to RADIUS messages during the authentication process.

Assessment

The Assessment Configuration defines the following requirements for end-system assessment:

- What assessment tests to run.

  The Assessment Configuration determines what types of assessment tests are executed and what parameters are used. For example, you can specify a Nessus assessment utilizing a specific Nessus configuration file that determines end-system compliance with the SANS Top 20 vulnerabilities. The same Nessus server can be used to assess Windows machines for Windows-related vulnerabilities and also assess MAC OS-based machines for MAC-related vulnerabilities. In addition, you can specify Nessus as well as other assessment services to jointly determine the security posture of a connecting device.

- What resources to use to run the assessment.

  The Assessment Configuration determines what assessment servers are used to perform the assessment. You can balance the assessment load between all your assessment servers, or you can select a specific assessment server pool to use. For example, assuming Nessus is chosen for assessment, end-systems connecting to the network in the company's headquarters can be assessed with the Nessus server deployed in the headquarters, while end-systems in a branch office will be assessed with Nessus servers deployed in the branch office, conserving bandwidth utilization on the network.

- How health results are processed.

  When an assessment is performed on an end-system, a "health result" is generated. For each health result, there may be several "health result details." A health result detail is a result for an individual test performed during the assessment. Each health result detail is given a score ranging from 1 to 10, and based on this score, the health result is assigned a risk level. However, it is possible to override the score with a different value that better aligns the score with the enterprise's compliance policy. For example, Wireshark is a popular network traffic analysis application that can be used for both informational and malicious intentions. If IT operations determines that Wireshark is an application that should not be installed on end-systems connecting to the network, a scoring override can be configured to associate a high-risk score if Wireshark is detected on an end-system.

- Which end-systems are quarantined.

  NAC Manager uses risk levels to determine whether or not an end-system will be quarantined. Based on the scores from the health result details, end-system are classified into one of four risk levels: high risk, medium risk, low risk, and no risk. Depending on the risk level to which the end-system is classified, the end-system may be quarantined.

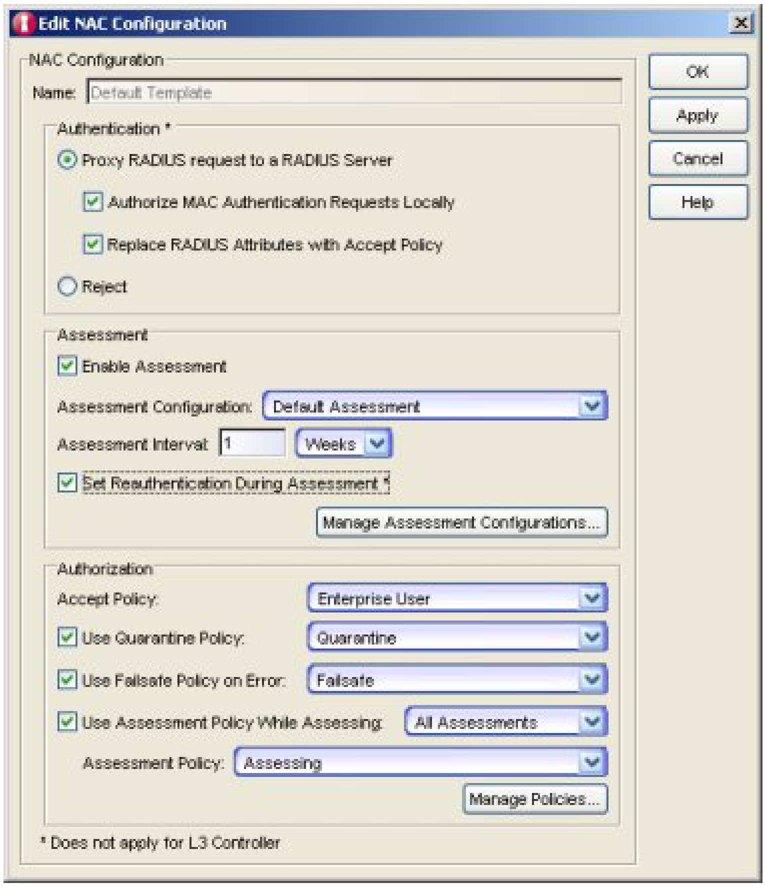
Authorization

The NAC configuration also specifies the authorization levels, referred to as "access policies," that will be applied to the end-system, depending on the authentication and assessment results.

- Accept Policy – the policy that is assigned to compliant end-systems.
- Quarantine Policy– the policy that is assigned to noncompliant end-systems that have failed assessment.
- Assessment Policy – the policy that is (optionally) assigned to end-systems while they are being assessed.
- Failsafe Policy – the policy that is assigned to end-systems when an error occurs in the NAC process.

The following figure shows the NAC Manager window used to create or edit a NAC Configuration and define its authentication, assessment, and authorization attributes.

Figure 5-3 NAC Configuration for a Security Domain



Edit NAC Configuration

NAC Configuration

Name: Default Template

Authentication *

● Proxy RADIUS request to a RADIUS Server

☑ Authorize MAC Authentication Requests Locally

☑ Replace RADIUS Attributes with Accept Policy

○ Reject

Assessment

☑ Enable Assessment

Assessment Configuration: Default Assessment

Assessment Interval: 1 Weeks

☑ Set Reauthentication During Assessment *

Authorization

Accept Policy: Enterprise User

☑ Use Quarantine Policy: Quarantine

☑ Use Failsafe Policy on Error: Failsafe

☑ Use Assessment Policy While Assessing: All Assessments

Assessment Policy: Assessing

* Does not apply for L3 Controller

The following table provides examples of various network scenarios that should be considered when identifying the number and configuration of Security Domains in your NAC deployment.

Table 5-1 Security Domain Configuration Guidelines

Network Scenario	Examples	Security Domain Configuration
Area of the network that is configured to authenticate end-systems with a secure authentication method, such as 802.1X or web-based authentication.	• Switches that provide access for trusted users authenticating to the network using 802.1X or web-based authentication, such as LAN segments and wireless networks designated for trusted user access. • VPN concentrator providing connectivity to users implementing remote access VPN to connect into the corporate LAN.	Proxy 802.1X and web-based authentication requests to a backend RADIUS server. This allows for the proper validation of end-system login credentials for 802.1X and web-based authentication methods. In NAC Manager, create a Security Domain with the following configuration attributes: • Select the “Proxy RADIUS Request to a RADIUS Server” radio button to allow the forwarding of RADIUS authentication requests to a RADIUS server. • If the RADIUS server returns a policy or VLAN based on user or end-system identity, uncheck “Replace RADIUS Attributes with Accept Policy.” Otherwise, user overrides can be configured to return a policy or VLAN based on the user or end-system. • Configure the Accept Policy with a policy or VLAN that allows less restrictive network access for trusted users.
Area of the network that is configured to MAC authenticate end-systems solely for the purpose of end-system detection.	• Switches that provide access to machine-centric end-systems, such as printers, IP phones, and IP cameras. • Switches that provide access to human-centric end-systems that are not authenticated in traditional network environments, such as untrusted users like guests and contractors.	Locally authorize MAC authentication attempts. This enables the detection and authorization of human-centric and machine-centric end-systems. In NAC Manager, create a Security Domain with the following configuration attributes: • With the “Proxy RADIUS Request to a RADIUS Server” radio button selected, check the “Authorize MAC Authentication Requests Locally” option and specify a policy or VLAN in the Accept Policy field. • Configure the Accept Policy field with a policy or VLAN that provides more restrictive network access for end-systems authenticating with a less secure authentication method.

Table 5-1 Security Domain Configuration Guidelines (continued)

Network Scenario	Examples	Security Domain Configuration
Area of the network that provides access to a group of users or devices that pose a potentially high risk to the security or stability of the network.	• Switches that provide access to guest users or contractors on a corporate network. These users are usually not directly under the administrative control of IT operations and pose additional risks to the network. • Switches that provide access to users within an organization that are allowed to engage in high risk behaviors on the network, or are not protected by security mechanisms such as a firewall or Intrusion Detection Systems (IDS). A sales organization that uses the Internet as a necessary part of their job, or a branch office location that is not protected by a firewall would both be characterized as high risk groups of users. • Wireless Access Points (APs) that are configured with an open wireless network or a wireless network that is secured through weak authentication/encryption mechanisms such as WEP. End-systems on these networks pose a greater risk to the organization because access to the network by untrusted users is easier.	Impose a more restrictive set of network resources in the authorization of connecting end-systems, and execute a thorough security posture assessment of connecting end-systems (if assessment is implemented on the network). These measures limit the network exposure to security threat propagation and protect against network instability. In NAC Manager, create a Security Domain with the following configuration attributes: • With the “Proxy RADIUS Request to a RADIUS Server” radio button selected, check the “Replace RADIUS Attributes with Accept Policy” option and specify a restrictive policy or VLAN in the Accept Policy field. Furthermore, a more extensive Assessment Configuration may be selected to scan these devices with a larger set of assessment parameters. This allows the administrator to locally authorize MAC authentication requests and overwrite the policy information returned from the RADIUS server with a more restrictive policy. • Configure the Accept Policy with a policy or VLAN that provides more restrictive network access for end-systems posing a higher risk.
Area of the network that is more apt to affect the network's overall security or stability.	• Switches that front-end a distribution layer device that often crashes in the event of security threats or other events on the network. Assigning a more restrictive policy to these end-systems protects against the instability of the infrastructure devices.	
Area of the network where authentication is not deployed and open network access is available.	• Switches that provide access to conference rooms, libraries, and other areas commonly used by untrusted users. • Access points that provide guest access to an open SSID.	

Table 5-1 Security Domain Configuration Guidelines (continued)

Network Scenario	Examples	Security Domain Configuration
Area of the network that is configured to allow access only to specific end-systems or users.	• Switches that provide access to only pre-configured end-systems and users in highly controlled environments, such as industrial automation networks.	For the NAC Gateway, reject all RADIUS authentication attempts. For the NAC Controller, set the Accept Policy to a highly restrictive policy or VLAN such as “Deny All.“ This allows the administrator to locally authorize specific MAC addresses or users by using MAC and user overrides, and rejecting all other connection attempts to the network.
Area of the network that provides access to a group of users or devices that pose a guaranteed low risk to the security and stability of the network.	• Switches that provide network access to servers that are highly protected from attack through the implementation of firewalls as well as network-based and host-based IDS. • Switches that provide network access to end-systems that are highly managed and restricted from risky network behaviors, such as end-systems that are restricted from Internet access and always kept up-to-date with the latest anti-virus and anti-malware definitions. This may include devices restricted to communication on the private LAN, and data center or network IT operations devices.	Authorize connecting end-systems with a less restrictive set of network resources, and either don’t implement assessment, or implement assessment less frequently and with fewer parameters. In NAC Manager, create a Security Domain with the following configuration attributes: • With the “Proxy RADIUS Request to a RADIUS Server” radio button selected, check the “Replace RADIUS Attributes with Accept Policy” option and specify a non-restrictive policy or VLAN in the Accept Policy field. This allows the administrator to locally authorize MAC authentication requests and overwrite the policy information returned from the RADIUS server with a less restrictive policy or VLAN. It should be noted that this configuration may open the network to security threats, and should be reviewed carefully before being implemented.
Area of the network that provides access to a group of users or devices that will be allocated a different set of network resources based on their location on the network.	• Switches that provide access to both trusted and untrusted users on the network, such as conference rooms and cafeterias. These areas can be configured to restrict trusted user access to servers containing sensitive information. This protects against the possibility that an untrusted user obtains access to a trusted user's computer that is logged into the network, or that an untrusted user eavesdrops on sensitive material being viewed by adjacent trusted users.	Impose the level of authorization based on requirements of IT operations. In NAC Manager, create a Security Domain with the following configuration attributes: • With the “Proxy RADIUS Request to a RADIUS Server” radio button selected, check the “Replace RADIUS Attributes with Accept Policy” option and specify a policy or VLAN in the Accept Policy field. This allows the administrator to locally authorize MAC authentication requests and overwrite the policy information returned from the RADIUS server with a different policy based on the network location of an end-system.

The following table provides network scenarios from an assessment standpoint that should be taken into account when identifying the number and configuration of Security Domains.

Table 5-2 Security Domain Configuration Guidelines for Assessment

Network Scenario	Examples	Security Domain Configuration
Area of the network, or a group of end-systems or users, that require end-system assessment with either the same set of assessment parameters, or a distinct set of parameters different from other areas of the network	• Switches that provide open access to the network, such as guest access areas. This requires that the Security Domain be associated to an Assessment Configuration that deeply scans connecting end-systems, since untrusted users are allowed access to the network. • Switches that provides access to trusted users on the network. This requires that the Security Domain be associated to an Assessment Configuration that scans for vulnerabilities common to applications and platforms utilized by trusted users, such as Windows XP and Microsoft Internet Explorer. • Switches that provide access to a specific group of devices (for example, IP phones and printers), devices running a specific set of applications (such as e-mail servers, web servers), or PCs running a specific OS (Microsoft 2003 Server, Microsoft XP, RedHat Linux, MAC OS). This requires that the Security Domain be associated to an Assessment Configuration that scans the connecting end-systems for vulnerabilities specific to the type of end-system. • A group of devices identified by MAC address, that are running a specific OS. This requires that a MAC override identifying these devices be associated to an Assessment Configuration that scans these connecting end-systems for vulnerabilities specific to the type of OS. • A group of devices identified by MAC address, that are a specific device type, such as printers or IP phones. This requires that a MAC override identifying these devices be associated to an Assessment Configuration that scans for vulnerabilities specific to the type of end-system, such as web servers with default login credentials. • Users, identified by username, that are identified as high risk personnel on the network. This requires that a user override identifying these users is associated to an Assessment Configuration that deeply scans these connecting end-systems for potentially malicious tools, applications, malware, and vulnerabilities.	Create an Assessment Configuration specifically configured to validate these security compliance parameters. In NAC Manager, create a Security Domain that uses this Assessment Configuration and leverages assessment servers configured to validate these security compliance parameters.

Table 5-2 Security Domain Configuration Guidelines for Assessment (continued)

Network Scenario	Examples	Security Domain Configuration
Area of the network, or a group of end-systems or users, that require assessment with immediate network access.	• Switches that provide network access to mission critical servers, mandating uninterrupted network connectivity while still implementing assessment. • Switches that provide network access to end-systems used by IT operations, requiring that network connectivity for debugging and troubleshooting is maintained during assessment. • Switches that provide network access to important end users such as executives, so network connectivity is maintained during assessment. • A group of devices, identified by MAC address, that are a specific OS or device type, such as printers or IP phones that require immediate network access upon connection. • Users identified by user name, that are identified as important personnel on the network and require immediate network access upon connection.	Do not use an Assessment Policy while end-systems are being assessed. This guarantees mission critical devices with time-sensitive network access maintain network availability during assessment. In NAC Manager, create a Security Domain with the following attribute: • The “Use Assessment Policy While Assessing” checkbox is not selected. In this case, NAC Manager assigns the policy or VLAN returned from the RADIUS server or the locally defined Accept Policy while the end-system is being assessed.
Area of the network, or group of end-systems or users, that require assessment before network access is allowed.	• Switches that provide access to untrusted users, such as guests or other high risk end-systems, may be configured to apply a highly restrictive Assessment Policy during end-system assessment, only permitting end-system communication to the assessment servers, as well as basic IP services such as ARP, DNS, and DHCP. Security threats created by these high-risk end-systems are mitigated by waiting until assessment is completed before authorizing a significant level of network access. • A group of devices, identified by MAC address, that are a specific OS or device type, and pose high risk to the network security. • Users, identified by username, that are identified as high risk personnel on the network.	Use an Assessment Policy during end-system assessment. In NAC Manager, create a Security Domain with the following attribute: • Select the “Use Assessment Policy While Assessing” checkbox and specify an Assessment Policy to assign.

3. Identify Required MAC and User Overrides

MAC and user overrides are used to handle end-systems that require a different set of authentication, assessment, and authorization parameters from the rest of the end-systems in a Security Domain. A MAC or user override can be defined within the scope of a specific Security Domain or all Security Domains. An override scoped to a specific Security Domain lets you specify how an end-system is authenticated, assessed, and authorized whenever the end-system connects to the network in that particular Security Domain. A global override lets you specify how an end-system is authenticated, assessed, and authorized whenever the end-system connects to any Security Domain on the network.

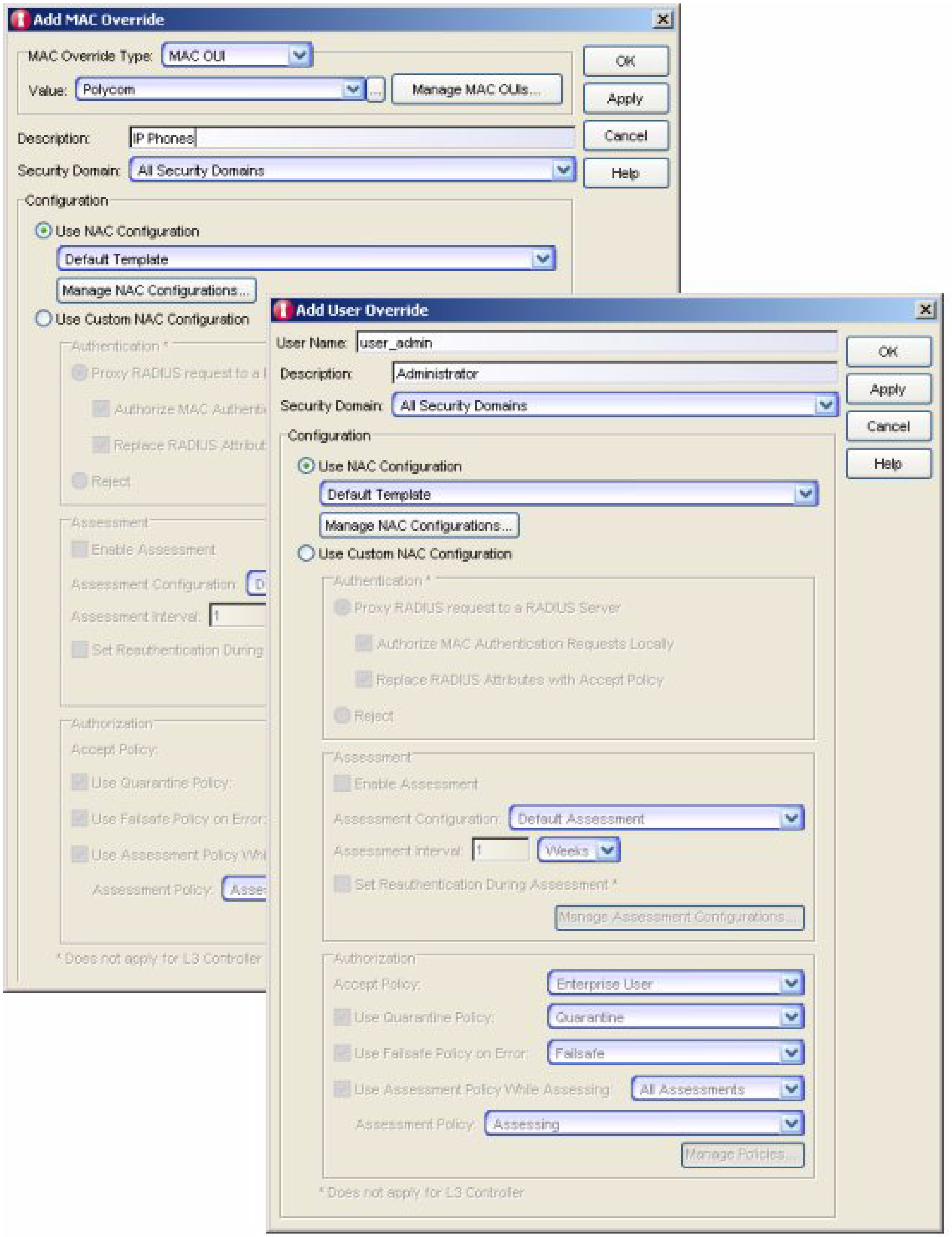
Use the network scenarios and examples provided in this section to determine what MAC and user overrides are required for your NAC deployment.

MAC Overrides

A MAC override lets you create a configuration for a single end-system (based on a full MAC address) or for a group of end-systems (based on a MAC OUI, a MAC OUI Group or a Custom MAC Mask). For example, you could create a MAC override that allocates VoIP services to certain IP phones based on a MAC OUI group. Or, you could deny a specific end-system by creating a MAC override that quarantines the MAC address of that end-system and restricts its network access.

The following figure displays the windows used for MAC and user override configuration in NAC Manager. Notice that either an existing NAC Configuration can be used or a custom configuration can be specified for the override.

Figure 5-4 MAC and User Override Configuration



Add MAC Override

MAC Override Type: MAC OUI

Value: Polycom

Description: IP Phones

Security Domain: All Security Domains

Configuration

● Use NAC Configuration: Default Template

○ Use Custom NAC Configuration

Add User Override

User Name: user_admin

Description: Administrator

Security Domain: All Security Domains

Configuration

● Use NAC Configuration: Default Template

○ Use Custom NAC Configuration

Assessment Configuration: Default Assessment

Assessment Interval: 1 Weeks

Accept Policy: Enterprise User

Use Quarantine Policy: Quarantine

Use Failsafe Policy on Error: Failsafe

Use Assessment Policy While Assessing: All Assessments

Assessment Policy: Assessing

Manage MAC OUIs...
OK
Apply
Cancel
Help
Manage NAC Configurations...
Authentication *
Proxy RADIUS request to a RADIUS Server
Authorize MAC Authentication Requests Locally
Replace RADIUS Attributes with Accept Policy
Reject
Assessment
Enable Assessment
Set Reauthentication During Assessment *
Manage Assessment Configurations...
Authorization
Manage Policies...
* Does not apply for L3 Controller

The following table describes scenarios where a MAC override may be configured for a particular end-system.

Table 5-3 MAC Override Configuration Guidelines

Network Scenario	Examples	Security Domain Configuration
A device, or class of devices, that utilize a distinct set of parameters for authentication, assessment, and authorization.	Allocating VoIP services to IP phones on the network. For example, you could create a MAC override where a Polycom IP Phone, identified by the MAC address OUI of the authenticating end-system, is assigned to the IP Phone policy or Voice VLAN and not assessed for security posture compliance when connecting to any Security Domain.	In NAC Manager, create a MAC override with the following attributes: • Specify either full MAC address or MAC address OUI. • Select the Security Domain or all Security Domains for the MAC override scope. For the assessment, authentication, and authorization configuration, choose a NAC Configuration or specify a custom configuration with the following parameters: • Select either the “Proxy RADIUS request to a RADIUS Server” radio button or the “Reject” radio button. • If the “Proxy RADIUS request to a RADIUS Server” radio button is selected, check “Authorize MAC Authentication Requests Locally” if MAC authentication requests are to be authorized, regardless of the MAC authentication password. • Check “Replace RADIUS Attributes with Accept Policy” if the policy information returned from the RADIUS server will be overwritten by the Accept Policy. • Format the Accept Policy with the policy or VLAN. • Check the “Enable Assessment” checkbox if this device, or class of devices, is to be assessed, and select the appropriate Assessment Configuration for these devices. • Specify the assessment and authorization parameters such as assessment interval, Quarantine Policy, and whether or not to apply the Assessment Policy while the end-system is being scanned.

Table 5-3 MAC Override Configuration Guidelines (continued)

Network Scenario	Examples	Security Domain Configuration
A device or class of devices needs to be restricted network access ("blacklisted") in a particular Security Domain or in all Security Domains.	Denying access or quarantining the MAC addresses of laptops used by guests or contractors in those areas of the network designated to provide access only to trusted employees.	In NAC Manager, create a MAC override with the following attributes: • Specify either full MAC address or MAC address OUI. • Select the Security Domain or all Security Domains for the MAC override scope. For the assessment, authentication, and authorization configuration, choose a NAC Configuration or specify a custom configuration with the following parameters: • Select either the "Proxy RADIUS request to a RADIUS Server" radio button or the "Reject" radio button. • Check "Authorize MAC Authentication Requests Locally" so MAC authentication attempts by these devices are assigned the Accept Policy. • Check "Replace RADIUS Policy with Accept Policy" so the policy information returned from the RADIUS server will be overwritten by the Accept Policy. • Select "Quarantine" as the Accept Policy. • Deselect the "Enable Assessment" checkbox so the end-systems are not assessed for security posture compliance Note that NetSight ASM leverages global ASM MAC overrides with this configuration to establish location-independent quarantine actions by quarantining end-systems that have violated the network security policy. To deny untrusted end-systems network access by sending the switch a RADIUS Access-Reject message (instead of quarantining), make the following change to the authorization configuration for the MAC override: • Select the "Reject" radio button instead of selecting the "Proxy RADIUS request to a RADIUS Server" radio button.

Table 5-3 MAC Override Configuration Guidelines (continued)

Network Scenario	Examples	Security Domain Configuration
A device, or class of devices, needs to be permitted a special level of network access (“whitelisted”) in a particular Security Domain or in all Security Domains.	Permitting an unrestricted level of access for end-systems that belong to IT operations.	In NAC Manager, create a MAC override with the following attributes: • Specify either full MAC address or MAC address OUI. • Select the Security Domain or all Security Domains for the MAC override scope. For the assessment, authentication, and authorization configuration, choose a NAC Configuration or specify a custom configuration with the following parameters: • Select the “Proxy RADIUS request to a RADIUS Server“ radio button. • Check “Authorize MAC Authentication Requests Locally“ so MAC authentication attempts by these devices are assigned the Accept Policy. • Check “Replace RADIUS Attributes with Accept Policy“ so the policy information returned from the RADIUS server will be overwritten by the Accept Policy. • Specify “Administrator“ as the Accept Policy to allow unlimited access for these devices. • Uncheck the “Enable Assessment“ checkbox so these devices are not assessed for security posture compliance.

User Overrides

A user override lets you create a configuration for a specific end user, based on the user name. For example, you could create a user override that gives a trusted end user immediate network access without performing an assessment.

User overrides can be used in network scenarios similar to those described for MAC overrides:

- A specific user that requires a distinct set of parameters for authentication, assessment, and authorization. For example, a user override can be configured for executives of a corporation to permit immediate network access without assigning the Assessment Policy during end-system assessment.
- A specific user can be restricted network access (“blacklisted”) for a particular Security Domain or all Security Domains, by associating the username with the Accept Policy of “Quarantine” or by sending a RADIUS Access-Reject for this user. For example, an employee can be restricted access to a certain area of the network, or students can be denied network access during an exam.
- A specific user can be permitted a special level of network access (“whitelisted”) by associating the username with the Accept Policy of “Administrator” to allow unlimited network access.

It is important to note that the Layer 3 NAC Controller may not determine the true MAC address of the downstream connected end-system. In this case, a MAC override configured in NAC

Manager will not match this end-system and the end-system is assigned the Security Domain's default NAC configuration. In addition, the Layer 3 NAC Controller is not able to determine the username associated to the downstream end-system for matching against user overrides, and the end-system is assigned the Security Domain's default NAC configuration.

Assessment Design Procedures

The following section provides the design procedures for implementing assessment in your NAC deployment.

1. Determine the Number of Assessment Servers

Assessment servers are used to implement assessment functionality in NAC deployments. Use the following parameters to determine the number of required assessment servers for your deployment:

- Load-sharing requirements.

  More than one assessment server may be required to handle the number of end-systems being assessed at any one time. The number of end-systems that can be assessed at the same time and the amount of time required to complete an assessment is determined by the number of vulnerabilities being assessed, throughput limitations on the network, and the hardware specifications of the assessment server machine. Load-sharing of end-system assessment is implemented in a round robin fashion between the assessment servers available in the assessment resource pool.

- Assessment server redundancy.

  To provide redundancy, at least two assessment servers should be configured per NAC deployment, with additional assessment servers added for load-balancing and scalability purposes.

The same assessment server can be used for multiple Security Domains, and each assessment server can assess end-systems using different sets of assessment parameters, depending on the device, user, or location is in the network. Here are some examples:

- If guests and other untrusted users are to be assessed for a different set of security vulnerabilities than trusted users, a Security Domain can be associated to the areas of the network where untrusted users connect, and can specify an Assessment Configuration that uses assessment servers configured for the assessment of untrusted users. If trusted users connect to this same Security Domain, another Assessment Configuration that leverages assessment servers configured to assess vulnerabilities of trusted users can be utilized. Note that if several Security Domains require the same assessment parameters, then these Security Domains can be configured to use the same Assessment Configuration.
- If a certain type of end-system (for example, an end-system of a particular model, having a particular OS, and running specific services) connects to the network in a certain area, or is identified by MAC address, a Security Domain and MAC override can be associated to this area of the network that uses an Assessment Configuration that leverages assessment servers that assess vulnerabilities specific to that type of end-system. For example, an area of the network where Microsoft IAS servers connect or where Polycom IP phones connect can be configured to utilize an assessment server configured to scan for Microsoft IAS web server-related vulnerabilities or Polycom IP phone default settings.

2. Determine Assessment Server Location

When determining the location of the assessment servers on the network, the following factors should be considered:

- The type of assessment: agent-less or agent-based.

  Agent-less assessment consumes more bandwidth than agent-based assessment during the scan of an end-system. However, it is important to understand that the amount of bandwidth consumed by agent-less assessment should only be considered when a large number of end-systems are being assessed over a severely bandwidth-restricted link. For example, if 1000 end-systems are connected to a branch office over a 512 Kbps connection that is also carrying latency-sensitive VoIP and other real-time applications, it is recommended to position an assessment server at the branch office to execute assessment for connecting devices and avoid congestion on the bandwidth restricted link.

- End-system configuration for the associated Security Domain.

  If agent-less assessment is implemented and connecting end-systems are running personal firewalls, the assessment server location may be relevant to the effectiveness of the assessments. For example, Microsoft XP SP2 is enabled by default with a personal firewall that denies all unsolicited inbound connection attempts. Therefore, a Microsoft XP SP2 personal firewall will prevent the successful execution of an end-system assessment unless the firewall is configured to allow specific types of unsolicited inbound connections, such as from specific IP addresses or over specific protocols as defined in the Exceptions list. This may be configured by the end user via web-based remediation or through a Windows domain controller group policy definition.

3. Identify Assessment Server Configuration

An assessment server utilizes third-party assessing software to execute scans against connecting end-systems, and this software must be locally configured with the security assessment parameters. The third-party assessing software on all assessment servers belonging to the same Security Domain must be configured identically so that consistency is maintained in the assessment of all connecting end-systems within that domain. The selection of the vulnerabilities assessed by the assessment servers is based solely on the enterprise security policy. Here are some examples of vulnerability assessment configuration:

- Remote scans that utilize a locally configured account on the end-system can evaluate virtually any configuration details of the end-system within the rights of the account. For an administrative account, any end-system parameters can be checked including the registry settings and the running services. Examples include the date of antivirus definition files, installation of antivirus software, status of antivirus protection, installed patches, and personal firewall status and configuration information.
- Remote scans that do not utilize a locally configured account on the end-system can evaluate a more limited set of vulnerabilities through the assessment of remotely accessible services on the end-system. Examples include OS-specific vulnerabilities accessed through open TCP/UDP ports and vulnerabilities of remotely-accessible services running on the end-system (FTP server, HTTP server).

The SANS Top 20 security vulnerabilities provide a suggested base guideline configuration for enterprises initially deploying NAC with end-system assessment (http://www.sans.org/top20/).

Third-party assessing software regularly releases updates to assess newly identified security vulnerabilities. A subscription to such a service is recommended to maintain an up-to-date assessment engine on the network. New vulnerabilities only need to be included in the assessment configuration if the security vulnerability is considered a risk for the organization. For more information on Nessus, refer to http://nessus.org/.

Out-of-Band NAC Design Procedures

The following section continues the Enterasys NAC design procedure with steps specifically relating to the implementation of out-of-band NAC with the NAC Gateway.

1. Identify Network Authentication Configuration

Since NAC Gateways utilize authentication for the detection of connecting end-systems, it is necessary to identify which authentication methods are to be configured in the intelligent edge of the network. For more information on evaluating authentication on the network, see "Survey the Network" (page 4-2).

The following considerations should be taken into account when deploying authentication on the network:

- The capabilities of end-systems connecting to the network.

  Human-centric devices may support user-based authentication methods such as 802.1X or web-based authentication only if an 802.1X supplicant or a web browser is supported on the end-system. Machine-centric devices most likely only support device-based authentication methods like MAC authentication.

- The types of users connecting to the network.

  It is necessary to understand how authentication affects the different type of users connecting to the network and what implications this has on the NAC solution. For example, while trusted users authenticate using a set of valid credentials held in a directory on the network, untrusted or guest users may fail authentication upon connection.

- The complexity involved in deploying authentication on the network, if it is not yet deployed.

  Rolling out 802.1X authentication on the network requires extensive planning and mandates configuration and possible upgrade of infrastructure devices and end-systems, and the dissemination of credentials to connecting users and devices. Since this is a significant undertaking, it may be desirable to utilize MAC-based authentication for the initial rollout of NAC and migrate over to 802.1X over a period of time. This way, most benefits of NAC can be obtained in the short term while the infrastructure is readied for a full 802.1X authentication rollout.

- The authentication method supported by the intelligent edge of the network.

  Edge infrastructure devices may need to support multiple authentication methods concurrently to account for different devices connecting to the network. Furthermore, the authentication and authorization of multiple devices on a single port may also need to be supported.

2. Determine the Number of NAC Gateways

The number of NAC Gateways to be deployed on the network is a function of the following parameters:

- The number of Security Domains configured on the network.

  Each NAC Gateway appliance may be associated to only one Security Domain. Therefore, the number of NAC Gateways deployed on the network will be greater than or equal to the number of Security Domains configured in NAC Manager. To support redundancy per Security Domain, at least two NAC Gateways must be deployed per Security Domain, as discussed below.

- The number of authenticating users and devices that are connected to each Security Domain.

  Each NAC Gateway appliance has the capability of supporting a maximum number of authenticating devices as shown in the following table:

Table 5-4 End-System Limits for NAC Gateways

NAC Gateway Model	Concurrent End-Systems Supported
NSTAG-FE100-TX	Up to 500
7S-NSTAG-01(-NPS)	Up to 1000
NSTAG-GE250-TX	Up to 1250
SNS-TAG-LPA	Up to 2000
SNS-TAG-HPA	Up to 3000
SNS-TAG-ITA	Up to 3000

  To roughly determine the number of required NAC Gateways per Security Domain, use the following formula:

  Number of authenticating end-systems in a Security Domain / Concurrent end-systems supported by gateway type = the number of required gateways of that type per Security Domain.

  For example, if you have 9000 end-systems connecting to a Security Domain, and you will be using SNS-TAG-ITA appliances, then the formula would be:

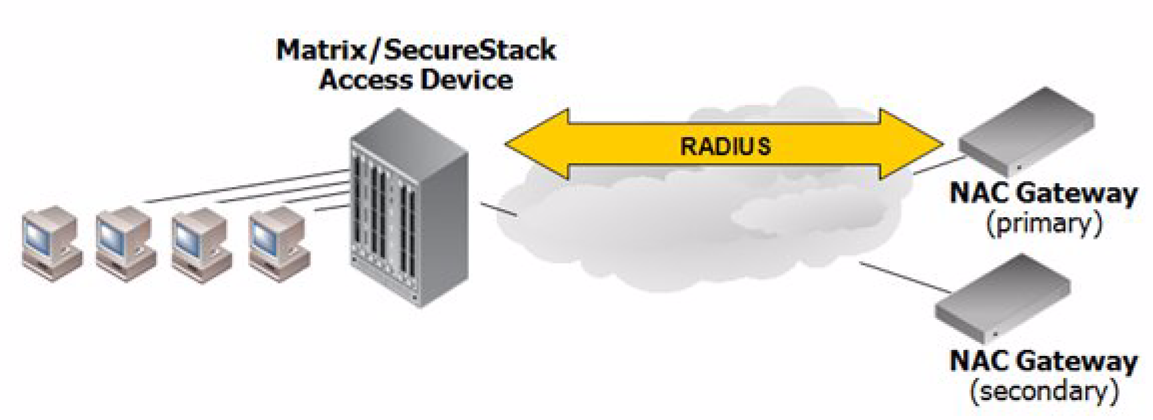
  9000 / 3000 = 3 required ITA appliances

  For each switch in a particular Security Domain, the maximum number of authenticating end-systems that may be connected to the switch at any one moment must be considered when associating a switch to a particular NAC Gateway appliance. Multiple intelligent switches residing in same Security Domain may be pointed to the same NAC Gateway, provided the maximum number of authenticating end-systems for the particular NAC Gateway is not exceeded. (Note that two switches in different Security Domains cannot be associated to the same NAC Gateway.)

- Configuration of NAC Gateway redundancy for each switch in a Security Domain.

  NAC Gateway redundancy for a particular switch is achieved by configuring two different NAC Gateways as primary and secondary RADIUS servers for that switch, as depicted in Figure 5-5 on page 5-21. When connectivity to the primary NAC Gateway is lost, the secondary NAC Gateway is used. Note that this configuration supports redundancy and not load-sharing, and the second NAC Gateway will only be used in the event that the primary NAC Gateway becomes unreachable.

Figure 5-5 NAC Gateway Redundancy



It is important that the secondary NAC Gateway does not exceed maximum capacity if the primary NAC Gateway fails on the network. For example, let's say that two NAC Gateways, both running at maximum load on the network, are being used by six switches. NAC Gateway #1 is the primary gateway for switch A, switch B, and switch C, and NAC Gateway #2 is the primary gateway for switch D, switch E, and switch F. In this scenario, NAC Gateway #1 should not be configured to serve as secondary for NAC Gateway #2 and vice versa. This is because if NAC Gateway #1 fails, NAC Gateway #2, which is already running at maximum capacity before NAC Gateway #1's failure, will not be able to handle the end-systems failing over from NAC Gateway #1. To avoid exceeding these limits, extra NAC Gateway appliances must be deployed on the network to serve as secondary NAC Gateways for these six switches.

To summarize, NAC Gateway redundancy may be accomplished using two different approaches:

- Active-standby redundancy

  In this redundancy approach, a set of switches are configured to use the same primary NAC Gateway (assuming these switches observe the NAC Gateway's capacity limitations previously described) and use the same secondary NAC Gateway as a backup (assuming the secondary NAC Gateway is the same model as the primary). The secondary NAC Gateway is not configured as a primary NAC Gateway for any switch on the network and therefore is inactive until a primary NAC Gateway fails. For example, if switch A, switch B, and switch C use NAC Gateway #1 as a primary gateway, then all three switches can be configured to use NAC Gateway #2 on the network as the backup. In this configuration, if switch A, switch B, or switch C loses connectivity to NAC Gateway #1, the switch would seamlessly transition to using NAC Gateway #2. In the worst-case scenario where all three switches lose connectivity to NAC Gateway #1, NAC Gateway #2 would be able to handle all authentication requests from these three switches. In this redundancy configuration, NAC Gateway #2 is completely idle on the network and only utilized if one of the switches cannot communicate to NAC Gateway #1.

- Active-active redundancy

  In this redundancy approach, the primary NAC Gateway for one switch is a secondary NAC Gateway for another switch. For this configuration, the same primary NAC Gateway is utilized for a group of switches, with this NAC Gateway running at only half the maximum load. Another group of switches utilizes a different primary NAC Gateway (assuming it is the same model) also running half the maximum load. Then, each group of switches can use the other NAC Gateway as the secondary gateway. This redundancy configuration guarantees that in the worst-case scenario, when all switches in one group lose communication to their primary NAC Gateway, the transition to the secondary NAC Gateway will not exceed maximum capacity.

To support redundancy within a Security Domain for either approach, one additional NAC Gateway (of the same model or with increased capacity) must be deployed per Security Domain in addition to the NAC Gateways deployed to handle the maximum number of concurrent end-systems connecting to the network.

It is important to note that each NAC Gateway can be configured to proxy RADIUS authentication requests to a particular RADIUS server. Therefore, if two switches in the network provide access to 802.1X or web-based authenticating users, and the credentials for the users connected to each switch are located on different RADIUS servers deployed on the network, then each switch must be configured to use its own NAC Gateway. Each NAC Gateway is then configured to use its respective RADIUS server. For example, an enterprise network that utilizes a particular RADIUS server for the 802.1X authentication of wireless users, would use a different RADIUS server for authenticating wired users. In this case, the same NAC Gateway could not be used for the switch providing wireless access and the switch providing wired access.

3. Determine NAC Gateway Location

After determining the number of NAC Gateways required for the NAC deployment, the next step is to determine NAC Gateway location on the network. This is dependent on the NAC deployment model that is implemented on the network.

If the NAC deployment does not implement remediation of quarantined end-systems or MAC (network) registration of new devices on the network, then the NAC Gateways are located in the authentication path of connecting end-systems as a proxy RADIUS server. This means that the RADIUS client on the access layer switches communicates directly to the NAC Gateway over UDP/IP, and the NAC Gateway in turn communicates to a backend RADIUS server. Therefore, the only requirement for NAC Gateway placement is that a routable IP forwarding path exists between each NAC Gateway and its associated access layer switches.

One option is to place all NAC Gateways in the data center, possibly adjacent to the RADIUS servers deployed on the network. Because the end-system assessment is not directly executed from the NAC Gateways, the choice of the location for the NAC Gateway does not impact the NAC operation, assuming IP connectivity between the access layer switches and the NAC Gateways is maintained.

For a branch office deployment of NAC, a NAC Gateway may be installed at the branch office or at the main site. The advantage of the NAC Gateway being installed at the branch office is that authentication traffic generated from end-systems at the branch office will not utilize the bandwidth of the WAN connection, unless authentication requests are proxied to a RADIUS server deployed at the main site. If the NAC Gateway is installed at the branch office location, NAC Manager requires communication to the NAC Gateway only during configuration, minimizing the bandwidth consumption over the WAN link. The NAC Gateway need not communicate with NAC Manager for the authentication, assessment, and authorization of connecting end-systems.

If either remediation or MAC registration is implemented, the NAC Gateways that are performing remediation and registration server functionality via web-redirection, must be strategically positioned on the network for end user notification. The NAC Gateway must be installed on a network segment directly connected to the router or routers that exist in the forwarding path for HTTP traffic from end-systems that may be quarantined or unregistered. This is because policy-based routing will be configured on the router or routers to redirect the web traffic sourced from quarantined and unregistered end-systems to the NAC Gateway to serve the remediation and registration web page.

It is important to note that only the NAC Gateways that are configured with remediation and registration functionality need to be positioned in such a manner. All other NAC Gateways may be positioned at any location on the network, with the only requirement being that access layer switches are able to communicate to the gateways. Typically, the NAC Gateway with remediation and registration functionality is positioned on a network segment directly connected to the distribution layer routers on the enterprise network, so that any HTTP traffic sourced from quarantined end-systems that are connected to the network's access layer can be redirected to that NAC Gateway. As an alternative, the NAC Gateway may be positioned on a network segment directly connected to the router providing connectivity to the Internet or internal web server farm. In this scenario, the HTTP traffic sourced from quarantined end-systems would be redirected to the NAC Gateway before reaching the Internet or internal web servers.

4. Identify Backend RADIUS Server Interaction

If a NAC Gateway is receiving 802.1X and/or web-based authentication requests for connecting end-systems, then a backend RADIUS server must be configured to validate end user credentials in the authentication process. For each NAC Gateway, a primary and secondary RADIUS server can be specified for the validation of user/device network login credentials on the network.

If 802.1X, web-based, or RADIUS authentication for switch management logins is implemented, a RADIUS server with backend directory services must be deployed on the network. A RADIUS server is not necessary if only MAC authentication is deployed on the network.

All RADIUS servers supporting RFC2865 and subsequent RADIUS standards are supported by Enterasys NAC appliances when proxying RADIUS authentication requests. Tests have been conducted on the following RADIUS servers:

- FreeRADIUS
- Microsoft IAS
- Funk Steelbelted RADIUS
- Cisco ACS

5. Determine End-System Mobility Restrictions

While Security Domain-specific MAC and user overrides can be configured to control end-system and end user mobility across the network and between Security Domains, the “Lock MAC” feature allows the network administrator to restrict network access for specific end-system to a switch port or switch. The end-system can be denied network access with a RADIUS Access-Reject message returned to the switch, or assigned a specific policy or VLAN when connecting to the network in a restricted area. Here are some examples of how the Lock MAC feature can be used:

- A printer, server, or other end-system could be allowed network access only when it is connected to a port specified by IT operations. This prevents security issues that could result if the device was moved to a different area of the network.
- An IP phone with a MAC override could be locked to a specific port on a switch. This would allow exact identification of the phone's location in case an emergency (911) call was placed from the phone.

6. VLAN Configuration

This step is for NAC deployments that use RFC-3580-compliant switches in the intelligent edge of the network to implement dynamic VLAN assignment of connecting devices.

NAC leverages VLAN Tunnel RADIUS attribute modification in RADIUS authentication messages for network resource allocation to end-systems connected to these RFC 3580-compliant switches. This requires that before NAC is deployed on the network, each RFC 3580-compliant switch in the intelligent edge of the network is configured with the appropriate VLANs that may be returned from the NAC Gateways. A list of VLANs that may be assigned to connecting end-systems for each Security Domain must be generated by analyzing the Accept Policy, Assessment Policy, Failsafe Policy, and Quarantine Policy of the following NAC configurations:

- The Security Domains’ default NAC configurations
- MAC overrides for the Security Domains
- User overrides for the Security Domains
- Global MAC and user overrides

7. Policy Role Configuration

This step is for NAC deployments that use Enterasys policy-enabled switches in the intelligent edge of the network to implement dynamic policy assignment of connecting devices.

NAC leverages Filter-ID RADIUS attribute modification in RADIUS authentication messages for network resource allocation to end-systems connected to these Enterasys switches. Therefore, before NAC is deployed on the network, each Enterasys switch in the intelligent edge of the network must be configured with the appropriate policy roles that may be returned from the NAC Gateways. A list of policy roles that may be assigned to connecting end-systems for each Security Domain can be generated by analyzing the Accept Policy, Assessment Policy, Failsafe Policy, and Quarantine Policy of the following NAC configurations:

- The Security Domains’ default NAC configuration
- MAC overrides for the Security Domains
- User overrides for the Security Domains
- Global MAC and user overrides

8. Define NAC Access Policies

Access policies define the authorization level that NAC assigns to a connecting end-system based on the end-system's authentication and/or assessment results. There are four access policies used in NAC Manager: Failsafe Policy, Accept Policy, Quarantine Policy, and Assessment Policy. In your security domain and override configurations, these access policies define a set of network access services that determine exactly how an end-system's traffic is authorized on the network.

When Enterasys policy-enabled switches are deployed in the intelligent edge of the network to authenticate and authorize connecting end-systems, these switches must be configured with access policies before NAC is deployed. NetSight Policy Manager enables the enterprise-wide deployment of policy roles to Enterasys policy-enabled switches, with a single click.

In addition to the enterprise's business specific roles, such as “Faculty” or “Sales,” NAC policy roles must be defined, configured, and enforced to the network for NAC. All policy roles previously specified in the NAC configuration must be defined in NetSight Policy Manager to ensure the consistent allocation of network resources to connecting end-systems.

Failsafe Policy and Accept Policy Configuration

The Failsafe Policy is assigned to end-systems when an error occurs in the NAC process. An error state results if the end-system's IP address could not be determined from its MAC address, or if there was an assessment error and an assessment of the end-system could not take place.

For Enterasys policy-enabled switches, a corresponding policy role (created in Policy Manager) should allocate a nonrestrictive set of network resources to the connecting end-system so it can continue its connectivity on the network, even though an error occurred in the NAC process.

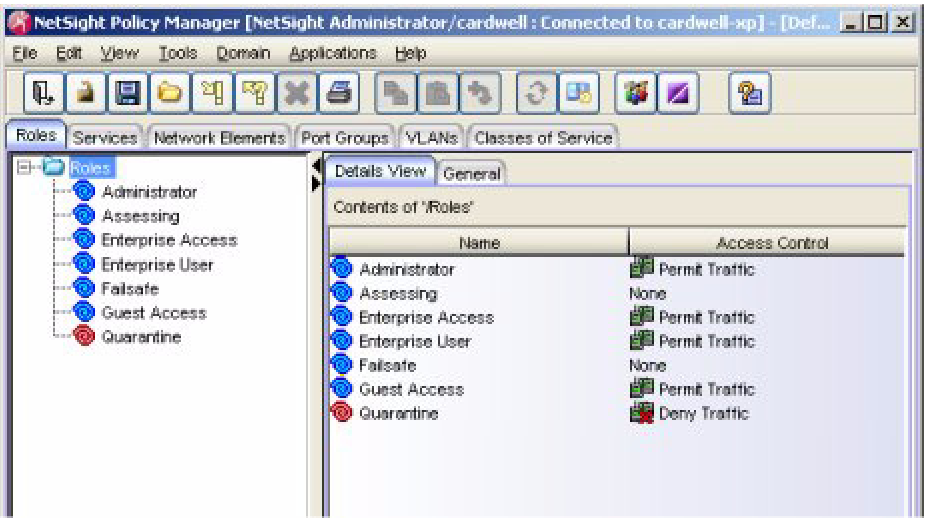
The Accept Policy is assigned to an end-system when it has been authorized locally by the NAC Gateway and when an end-system has passed an assessment (if an assessment was required), or if the Accept Policy has been configured to replace the Filter-ID information returned in the RADIUS authentication messages.

For Enterasys policy-enabled switches, a corresponding policy role (created in Policy Manager) would allocate the appropriate set of network resources for the end-system depending on their role in the enterprise. For example, you might associate the Accept Policy to the “Enterprise User” role that is defined in the NetSight Policy Manager demo.pmd file.

Assessment Policy and Quarantine Policy Configuration

The Assessment Policy and Quarantine Policy are used when end-system assessment is implemented in the NAC deployment. The policy roles shown in the Policy Manager window below correspond to the access policies used in NAC Manager. For example, the Assessing Policy role in Policy Manager corresponds to the Assessment Policy in NAC Manager. Note that the Administrator, Enterprise User, Enterprise Access, and Guest Access policy roles are also defined in the Policy Manager demo.pmd file.

Figure 5-6 Policy Role Configuration in NetSight Policy Manager


NetSight Policy Manager [NetSight Administrator/cardwell : Connected to cardwell-xp] - [Def...
File Edit View Tools Domain Applications Help
Roles Services Network Elements Port Groups VLANs Classes of Service
Roles
Administrator
Assessing
Enterprise Access
Enterprise User
Failsafe
Guest Access
Quarantine
Details View General

Contents of '/Roles'

Name	Access Control
Administrator	Permit Traffic
Assessing	None
Enterprise Access	Permit Traffic
Enterprise User	Permit Traffic
Failsafe	None
Guest Access	Permit Traffic
Quarantine	Deny Traffic

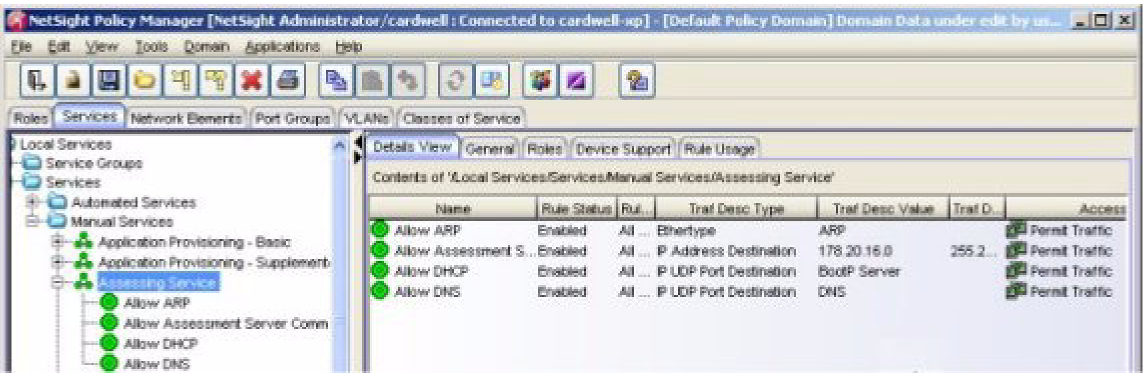
Assessment Policy

The Assessment Policy may be used to temporarily allocate a set of network resources to end-systems while they are being assessed. For Enterasys policy-enabled switches, a corresponding policy role (created in Policy Manager) should allocate the appropriate set of network resources needed by the assessment server to successfully complete its end-system assessment, while restricting the end-system's access to the network. For example, if the assessment server is configured to scan for FTP vulnerabilities, and the Assessment Policy does not allow FTP traffic from the end-system onto the network, then the assessment server will not detect the FTP vulnerabilities on the end-system.

To achieve this trade off, the Assessing policy role can be configured by default to deny all traffic, and be associated to classification rules that permit traffic to all assessment servers, using destination IP address Permit classification rules, as shown in Figure 5-7. Therefore, all traffic involved with the end-system's assessment is allowed onto the network. In addition, other basic network services such as ARP, DHCP, and DNS are allowed onto the network so the end-system can establish IP connectivity in the network while being assessed.

The Assessment Policy can also be configured to implement web notification during the execution of the assessment, to inform the end user that access to the network has been temporarily restricted while the assessment takes place. This is implemented by allowing HTTP traffic onto the network in addition to the other services previously described.

Figure 5-7 Service for the Assessing Role



NetSight Policy Manager [NetSight Administrator/cardwell : Connected to cardwell-xp] - [Default Policy Domain] Domain Data under edit by us...

Contents of '/Local Services/Services/Manual Services/Assessing Service'

Name	Rule Status	Rul...	Traf Desc Type	Traf Desc Value	Traf D...	Access
Allow ARP	Enabled	All ...	Ethertype	ARP		Permit Traffic
Allow Assessment S...	Enabled	All ...	IP Address Destination	178.20.16.0	255.2...	Permit Traffic
Allow DHCP	Enabled	All ...	IP UDP Port Destination	BootP Server		Permit Traffic
Allow DNS	Enabled	All ...	IP UDP Port Destination	DNS		Permit Traffic

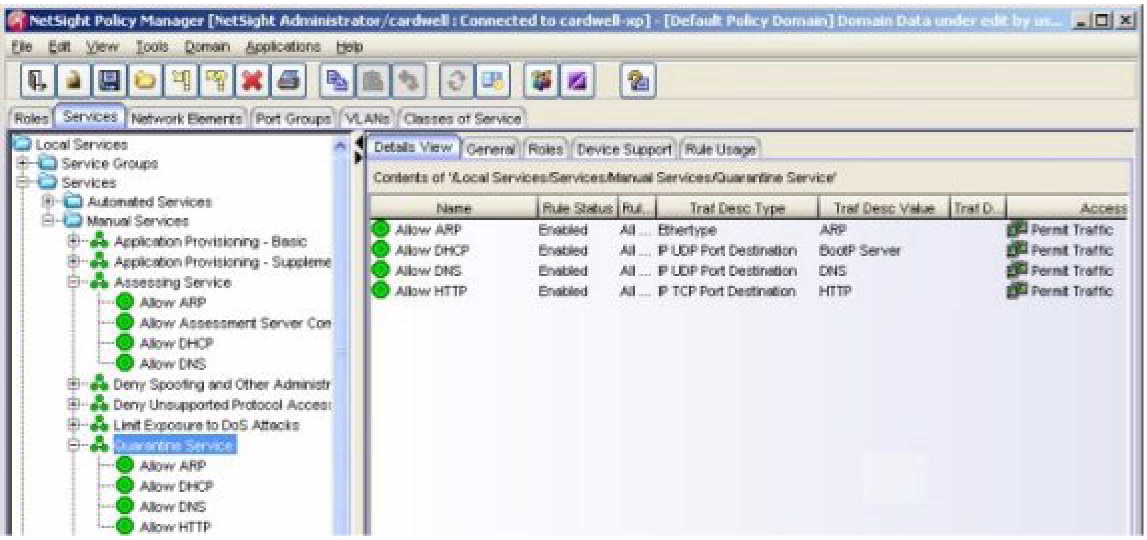
Note that it is not mandatory to assign the Assessment Policy to a connecting end-system while it is being assessed. NAC can be configured to assign the policy role received from the RADIUS server or the Accept Policy to the end-system while it is being assessed. In this way, the end-system can be granted immediate network access without mandating that the end user wait for assessment to be complete before full network resource allocation is granted. If NAC is configured to return the policy role received from the RADIUS Server, it is necessary that the enterprise's business-specific policy roles are configured to allow access to the appropriate network resources for communication with the assessment servers during assessment. This can be implemented by associating the Assessing service shown in Figure 5-7 to all business-specific policy roles in the NetSight Policy Manager configuration.

Quarantine Policy

The Quarantine Policy is used to restrict network access to end-systems that have failed assessment. For Enterasys policy-enabled switches, a corresponding Quarantine policy role (created in Policy Manager) should deny all traffic by default while permitting access to only required network resources such as basic network services (ARP, DHCP, and DNS).

If the NAC deployment implements remediation, the services associated to the Quarantine Policy must be configured to allow all HTTP traffic onto the network, in addition to other basic IP services such as ARP, DNS, and DHCP as shown in Figure 5-8.

Figure 5-8 Service for the Quarantine Role



- Local Services
  - Service Groups
  - Services
    - Automated Services
    - Manual Services
      - Application Provisioning - Basic
      - Application Provisioning - Suppleme
      - Assessing Service
        - Allow ARP
        - Allow Assessment Server Con
        - Allow DHCP
        - Allow DNS
      - Deny Spoofing and Other Administr
      - Deny Unsupported Protocol Acces
      - Limit Exposure to DoS Attacks
      - Quarantine Service
        - Allow ARP
        - Allow DHCP
        - Allow DNS
        - Allow HTTP

Contents of '/Local Services/Services/Manual Services/Quarantine Service'

Name	Rule Status	Rul...	Traf Desc Type	Traf Desc Value	Traf D...	Access
Allow ARP	Enabled	All ...	Ethertype	ARP		Permit Traffic
Allow DHCP	Enabled	All ...	IP UDP Port Destination	BootP Server		Permit Traffic
Allow DNS	Enabled	All ...	IP UDP Port Destination	DNS		Permit Traffic
Allow HTTP	Enabled	All ...	IP TCP Port Destination	HTTP		Permit Traffic

Furthermore, the Quarantine Policy and other network infrastructure devices must be configured to implement HTTP traffic redirection for quarantined end-systems to return web notification of the quarantined state of an end-system.

Unregistered Policy

If MAC (network) registration is configured in the NAC deployment, an "Unregistered" policy can be assigned to connecting end-systems while they are unregistered on the network. This policy must be configured to allow basic services such as ARP, DNS, DHCP, and to implement HTTP traffic redirection to return web-based notification for unregistered end-systems. (Because this configuration is similar to the Quarantine Policy and the Assessment Policy, those policies could be assigned to unregistered end-systems, if desired).

Inline NAC Design Procedures

The following section continues the Enterasys NAC design procedure with steps specifically relating to the implementation of inline NAC with the NAC Controller.

1. Determine NAC Controller Location

Because the NAC Controller is placed inline with traffic sourced from connecting end-systems, the location of NAC Controllers is directly dependent on the network topology. NAC Controllers are typically placed between the edge where end-systems connect to the network (for example, the wired and wireless access edge, or the remote access edge behind a VPN concentrator) and the network's core and data center where mission critical infrastructure resources reside. This way, noncompliant end-systems can be restricted from communicating to mission critical resources.

With the NAC Controller acting as the authorization point for traffic enforcement with inline NAC, there is a fundamental trade-off when positioning the NAC Controller in the network topology: the closer the NAC Controller is placed to the edge of the network, the higher the level of security is achieved, in that end-systems are authorized closer to the point of connection and end-systems deemed noncompliant have access to a smaller set of network resources.

However, the closer the NAC Controller is placed to the edge of the network, the more NAC Controllers are required on the network, increasing NAC deployment cost and complexity. Conversely, when moving the NAC Controller towards the core of the network, fewer NAC Controllers are required, decreasing NAC deployment cost and complexity, but also decreasing the level of security.

For implementing NAC on wired and wireless LANs, it is recommended that the Layer 2 NAC Controller is positioned between the access layer and distribution layer before the first routed hop in the network. As an alternative, the NAC Controller may be positioned deeper into the network after the first routed hop using the Layer 3 configuration. The Layer 3 NAC Controller can also be positioned after a VPN concentrator or WAN connection to implement NAC for remote users.

Unlike the out-of-band NAC design, the implementation of remediation and/or MAC (network) registration does not affect the location of the NAC Controller. The NAC Controller will appropriately intercept web traffic for the purpose of remediation and registration.

Lastly, it should be understood that some advantages exist with the deployment of a Layer 2 NAC Controller over a Layer 3 NAC Controller, which may affect the decision of how NAC Controllers are positioned. While a Layer 2 NAC Controller always knows the MAC address of the downstream connected end-system, the Layer 3 NAC Controller may not be able to determine the MAC address of a downstream end-system (denoted as “Unknown” in NAC Manager.) Techniques such as NetBIOS lookups and DHCP snooping are implemented to attempt to resolve the IP address of the downstream connected end-systems; however, scenarios exist where the IP address of the downstream end-system may not be determined.

The MAC address of a downstream end-system will be determined by the NAC Controller in the following scenarios:

- End-systems support NetBIOS and a host firewall does not drop inbound NetBIOS requests for the LAN connection.
- DHCP is implemented and the DHCP server exists upstream from the NAC Controller.

Since the Layer 3 NAC Controller may not be able to determine the MAC address of a downstream end-system, “Lock MAC” and MAC overrides are not applicable to Layer 3 NAC Controllers. Furthermore, MAC (network) registration may not be implemented when the MAC address of a downstream connected end-system is unknown. In this case, the end-system is assigned the Security Domain’s default NAC configuration.

2. Determine the Number of NAC Controllers

The number of NAC Controllers to be deployed on the network is a function of the following parameters:

- The network topology.

  Because the NAC Controller is placed inline with traffic sourced from connecting end-systems, the number of NAC Controllers required is directly dependent on the network topology. After the location of the NAC Controller is identified from the network topology, the minimum number of NAC Controllers can be determined.

- The number of Security Domains configured on the network.

  Each NAC Controller can be associated to only one Security Domain. Therefore, the number of NAC Controllers deployed on the network will be greater than or equal to the number of Security Domains configured in NAC Manager. To support redundancy per Security Domain, at least two NAC Controllers must be deployed per Security Domain, as discussed below.

- The number of users and devices that are connected to each Security Domain.

  Each NAC Controller appliance has the capability of supporting up to 2000 end-systems connected downstream as shown in the following table.

Table 5-5 End-System Limits for NAC Controllers

NAC Controller Model	Concurrent End-Systems Supported
7S4280-19-SYS	Up to 2000
2S4082-25-SYS	Up to 2000

  To identify the minimum number of NAC Controllers required to support inline NAC, use the following formula:

  Number of connecting end-systems in a Security Domain / Concurrent end-systems supported by controller type = the number of required NAC Controllers of that type, per Security Domain.

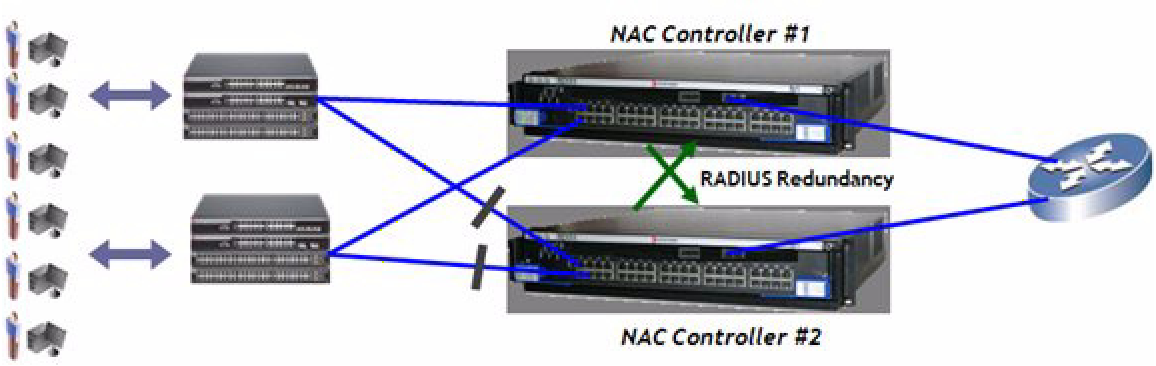
- The configuration of NAC Controller redundancy.

  To achieve redundancy at each location in the network where the NAC Controller is positioned, an additional NAC Controller is required, essentially doubling the total number of required NAC Controllers. Redundancy implementation differs between Layer 2 and Layer 3 Controllers.

  For a Layer 2 NAC Controller, redundancy is achieved in two different ways. Redundancy for the NAC Policy Enforcement Point (PEP) component of the NAC Controller is achieved by implementing 802.1w/s spanning tree between the redundant NAC Controllers as shown in Figure 5-9 on page 5-31. Redundant Layer 2 NAC Controllers are active-passive when only one spanning tree for one VLAN is configured between the NAC Controllers, and are active-active when multiple spanning trees for multiple VLANs are configured between the redundant NAC Controllers. If NAC Controller #1's Policy Enforcement Point (PEP) stops forwarding traffic, the network will automatically converge via 802.1w/s spanning tree to forward traffic through NAC Controller #2.

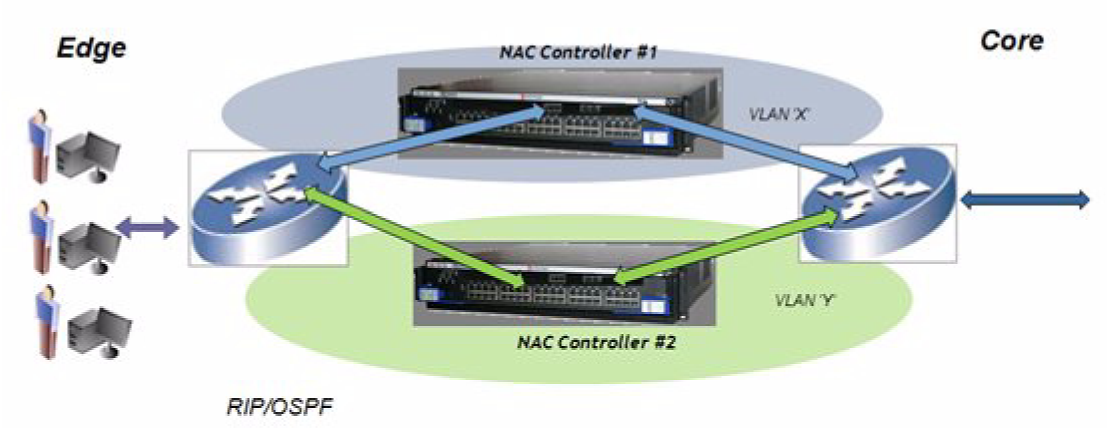
  Redundancy for the NAC Engine component of the NAC Controller is achieved by the redundant NAC Controllers using each other as backup RADIUS servers. If NAC Controller #1's Engine stops processing RADIUS authentication requests, the redundant NAC Engine will take over processing RADIUS messages as shown in Figure 5-9 on page 5-31.

Figure 5-9 Layer 2 NAC Controller Redundancy



For a Layer 3 NAC Controller, redundancy is achieved by implementing redundant Layer 3 NAC Controllers on adjacent, but separate networks as shown in Figure 5-10. The NAC Controllers must be in different networks, and a dynamic routing protocol such as OSPF or RIP must be configured between the upstream and downstream routers that are positioned on either side of the NAC Controllers. Redundant Layer 3 NAC Controllers are active-active, in that traffic from a downstream router may pass through either of the redundant Layer 3 NAC Controllers with equal cost multipath forwarding implemented for the configured dynamic routing protocol. If NAC Controller #1 (PEP or NAC Engine) stops forwarding traffic, the network will automatically converge using the configured routing protocol to forward traffic through NAC Controller #2. Note that the NAC Controllers do not route packets and do not participate in the layer 3 topology.

Figure 5-10 Layer 3 NAC Controller Redundancy



3. Identify Backend RADIUS Server Interaction

Layer 2 NAC Controllers detect downstream end-systems via authentication: MAC, web-based, or 802.1X. If web-based or 802.1X authentication is implemented, then a backend RADIUS server must be configured to validate end user credentials in the authentication process. For each Layer 2 NAC Controller, primary and secondary RADIUS servers may be specified for the validation of user/device network login credentials on the network.

4. Define Policy Configuration

Policies are assigned to downstream end-systems on the NAC Controller to authorize connecting devices with a level of network access. A default set of policies are automatically configured on each NAC Controller after installation and initialization of the appliance. This set of policies includes all policies defined by default in NAC Manager, such as Enterprise User, Quarantine, Assessing, Unregistered, and Failsafe. It is strongly recommended that the policy configurations of all NAC Controllers are imported into NetSight Policy Manager, reviewed, and appropriately modified, prior to the full rollout of inline NAC.

Failsafe Policy and Accept Policy Configuration

The Failsafe Policy is assigned to end-systems when an error occurs in the NAC process. The Failsafe policy role is configured by default on the NAC Controller to be used as the Failsafe Policy in NAC Manager. This policy is restrictive, allowing DNS and DHCP, and redirecting web traffic to serve back a web page stating an error has occurred on the network, while discarding all other types of traffic.

If it is desired to open network access when an error is encountered, the Enterprise User policy role can be selected as the Failsafe Policy in the NAC Configuration. The Enterprise User policy role is fairly open, permitting most types of communication onto the network. For security purposes the Enterprise User policy role does deny communication to the NAC Controller over TCP and UDP ports (utilized for administrative purposes, such as RADIUS and SSH). In addition, the Enterprise User policy discards all communication to NAC Manager's IP address for further security hardening. This policy role can be altered to further control which services a compliant end-system is allowed to utilize.

The Accept Policy is assigned to end-systems when they are deemed compliant. The Enterprise User policy role is configured by default on the NAC Controller to be used as the Accept Policy in NAC Manager.

Assessment Policy and Quarantine Policy Configuration

The Assessment Policy and Quarantine Policy are used when end-system assessment is implemented in the NAC deployment. The Assessment Policy may be used to temporarily allocate a set of network resources to end-systems while they are being assessed. The Assessing policy role is configured by default on NAC Controllers to be used as the Assessment Policy in NAC Manager. This policy allows DNS and DHCP, and any traffic destined to the IP address of the assessment servers deployed on the network. The policy also redirects web traffic to serve back a web page stating that the end-system has been restricted access while its security posture is being determined. All other types of traffic are discarded.

If it is desired to open network access while an end-system is being assessed, the use of the Assessment Policy can be disabled in the NAC configuration, or the Enterprise User policy role can be selected as the Assessment Policy instead. It is important to note that whenever a NAC configuration is enforced to the NAC Controller, the Assessment Policy is configured to allow assessment servers to reach the end-system while it is being assessed, regardless of whether the Assessing policy, Enterprise User policy, or any other policy role is utilized for assessment.

The Quarantine Policy is used to restrict network access to end-systems that have failed assessment. The Quarantine policy role is configured by default on the NAC Controller to be used as the Quarantine Policy in NAC Manager. This policy is restrictive, allowing DNS and DHCP, and redirecting web traffic to serve back a web page stating the end-system has been restricted access because it is deemed noncompliant. All other types of traffic are discarded. If it is desired to open network access when an end-system fails the assessment, the use of the Quarantine Policy can be disabled in the NAC Configuration or the Enterprise User policy role can be selected as the Quarantine Policy.

Unregistered Policy

If MAC (network) registration is to be configured on Layer 2 NAC Controllers, the Unregistered policy role configured by default on the NAC Controller can be used for the Accept Policy of unregistered devices. This policy is restrictive, allowing DNS and DHCP, and redirecting web traffic to serve back a registration web page stating the end-system has been restricted access because it has not yet registered. All other types of traffic are discarded.

Additional Considerations

This section presents additional design considerations for both inline and out-of-band NAC deployments.

NAC Deployment With an Intrusion Detection System (IDS)

NAC deployments that implement end-system assessment complement networking environments with IDS technologies that detect real-time security events on the network. While end-system assessment determines the security posture of connecting devices and mitigates threats posed by vulnerable end-systems, it does not determine the end user's intentions, whether malicious or benevolent. Therefore, IDS technologies can monitor how an end-system utilizes network resources after NAC has validated the security posture compliance of the end-system.

However, end-system assessments utilized in NAC may be classified by an IDS (depending on its configuration) as an attack. Therefore, if the traffic from the assessment server traverses a network link that is monitored by an IDS sensor, the IDS must be configured to not generate security events for traffic sourced from the assessment server’s IP address. The same applies for IPS systems.

NAC Deployment With NetSight ASM

NetSight ASM can be configured to notify the locally installed NAC Manager to dynamically configure a MAC override for a threat MAC address on the network. When a security threat is detected on the network, either through Enterasys Dragon IDS or a third-party device, and the security threat is communicated to NetSight ASM for an automated response, ASM can then quarantine the source of the attack at the port of connection using policy, and also communicate this quarantine action to NAC. If the end-system sourcing the security threat moves to a different port on the network, the end-system will remain quarantined, due to a dynamically configured MAC override, to protect the network from the possibility of future attacks. Therefore, the deployment of NAC not only proactively protects the network from security threats posed by vulnerable end-systems, but it also empowers the network's dynamic response characteristics to real-time threats detected from end-systems.